

simple + secure

Sophos UTM

administratorhandbuch

Produktversion: 9.200

Erstellungsdatum: Mittwoch, 19. Februar 2014



Einschränkung der Gewährleistung

Für die Richtigkeit des Inhalts dieses Handbuchs wird keine Garantie übernommen. Hinweise auf Fehler und Verbesserungen nehmen wir gerne unter der E-Mail-Adresse nsg-docu@sophos.com entgegen.

Inhaltsverzeichnis

1 Installation 15

1.1 Empfohlene Lektüre 15
1.2 Systemanforderungen 16
1.2.1 USV-Unterstützung 17
1.2.2 RAID-Unterstützung 17
1.3 Installationsanleitung 17
1.3.1 Tastenfunktionen während der Installation 18
1.3.2 Besondere Optionen während der Installation 18
1.3.3 Installation vonSophos UTM 19
1.4 Grundkonfiguration 22
1.5 Backup-Wiederherstellung 28

2 WebAdmin 31

2.1 WebAdmin-Menü 32
2.2 Symbolleiste 33
2.3 Listen 34
2.4 Suche in Listen 35
2.5 Dialogfelder 37
2.6 Schaltflächen und Symbole 38
2.7 Objektlisten 40

3 Dashboard 41

3.1 Dashboard-Einstellungen 43
3.2 Flow-Monitor 45

4 Verwaltung 49

4.1 Systemeinstellungen 50
4.1.1 Organisatorisches 50
4.1.2 Hostname 50
4.1.3 Zeit und Datum 50
4.1.4 Shell-Zugriff 53
4.1.5 Scan-Einstellungen 55
4.1.6 Zurücksetzung 55
4.2 WebAdmin-Einstellungen 57
4.2.1 Allgemein 57
4.2.2 Zugriffskontrolle 58
4.2.3 HTTPS-Zertifikat 59
4.2.4 Benutzereinstellungen 61
4.2.5 Erweitert 62

4.3 Lizenzen 64
4.3.1 Erwerb einer Lizenz 65
4.3.2 Lizenzmodell 66
4.3.3 Übersicht 71
4.3.4 Installation 71
4.3.5 Aktive IP-Adressen 72
4.4 Up2Date 72
4.4.1 Übersicht 73
4.4.2 Konfiguration 75
4.4.3 Erweitert 76
4.5 Backup/Wiederherstellen 77
4.5.1 Backup/Wiederherstellen 77
4.5.2 Automatische Backups 81
4.6 Benutzerportal 82
4.6.1 Allgemein 85
4.6.2 Erweitert 85
4.7 Benachrichtigungen 87
4.7.1 Allgemein 87
4.7.2 Benachrichtigungen 88
4.7.3 Erweitert 88
4.8 Anpassungen 89
4.8.1 Allgemein 89
4.8.2 Web-Meldungen 91
4.8.2.1 Web-Meldung ändern 93
4.8.2.2 Download-Verwaltung 93
4.8.3 Web-Vorlagen 95
4.8.3.1 Web-Vorlagen anpassen 95
4.8.3.2 Benutzerspezifische Web-Vorlagen und Bilder hochladen 96
4.8.4 E-Mail-Mitteilungen 97
4.9 SNMP 97
4.9.1 Anfrage 98
4.9.2 Traps 100
4.10 Zentrale Verwaltung 101
4.10.1 Sophos UTM Manager 101
4.11 High Availabilty (Hochverfügbarkeit) 104
4.11.1 Hardware- und Software-Voraussetzungen 106
4.11.2 Status 106
4.11.3 Systemstatus 108
4.11.4 Konfiguration 108
4.12 Ausschalten/Neustart 112

5 Definitionen & Benutzer 115

5.1 Netzwerkdefinitionen 115
5.1.1 Netzwerkdefinitionen 116
5.1.2 MAC-Adressdefinitionen 121
5.2 Dienstdefinitionen 122
5.3 Zeitraumdefinitionen 124
5.4 Benutzer & Gruppen 125
5.4.1 Benutzer 126
5.4.2 Gruppen 129
5.5 Client-Authentifizierung 132
5.6 Authentifizierungsdienste 134
5.6.1 Allgemein 134
5.6.2 Server 136
5.6.2.1 eDirectory 136
5.6.2.2 Active Directory 138
5.6.2.3 LDAP 141
5.6.2.4 RADIUS 143
5.6.2.5 TACACS+ 145
5.6.3 Single Sign-On 146
5.6.4 Einmaliges Kennwort (OTP) 148
5.6.5 Erweitert 153
6 Schnittstellen & Routing 157
6.1 Schnittstellen 157
6.1.1 Schnittstellen 158
6.1.1.1 Automatische Netzwerkschnittstellen-Definitionen 159
6.1.1.2 Arten von Schnittstellen 159
6.1.1.3 Gruppe 161
6.1.1.4 3G/UMTS 162
6.1.1.5 Ethernet-Statisch 164
6.1.1.6 Ethernet-VLAN 166
6.1.1.7 Ethernet-DHCP 168
6.1.1.8 DSL (PPPoE) 170
6.1.1.9 DSL (PPPoA/PPTP) 173
6.1.1.10 Modem (PPP) 175
6.1.2 Zusätzliche Adressen 178
6.1.3 Linkbündelung 179
6.1.4 Uplink-Ausgleich 180
6.1.5 Multipathregeln 184
6.1.6 Hardware 187
6.2 Bridging 188
6.2.1 Status 189

6.2.2 Erweitert 190
6.3 Dienstqualität (QoS) 191
6.3.1 Status 192
6.3.2 Verkehrskennzeichner 193
6.3.3 Bandbreiten-Pools 198
6.3.4 Download-Drosselung 200
6.3.5 Erweitert 201
6.4 Uplink-Überwachung 202
6.4.1 Allgemein 202
6.4.2 Aktionen 203
6.4.3 Erweitert 204
6.5 IPv6 206
6.5.1 Allgemein 207
6.5.2 Präfix-Bekanntmachungen 207
6.5.3 Umnummerierung 209
6.5.4 6to4 210
6.5.5 Tunnel-Broker 210
6.6 Statisches Routing 212
6.6.1 Statische Routen 212
6.6.2 Richtlinienrouten 214
6.7 Dynam. Routing (OSPF) 215
6.7.1 Allgemein 216
6.7.2 Bereich 217
6.7.3 Schnittstellen 219
6.7.4 Prüfsummen 221
6.7.5 Fehlersuche 221
6.7.6 Erweitert 222
6.8 Border Gateway Protocol 223
6.8.1 Allgemein 224
6.8.2 Systeme 224
6.8.3 Neighbor 225
6.8.4 Routemap 227
6.8.5 Filterliste 229
6.8.6 Erweitert 230
6.9 Multicast Routing (PIM-SM) 231
6.9.1 Allgemein 232
6.9.2 Schnittstellen 233
6.9.3 RP-Router 234
6.9.4 Routen 235
6.9.5 Erweitert 236

7 Netzwerkdienste 237

7.1 DNS 237
7.1.1 Allgemein 237
7.1.2 Weiterleitung 238
7.1.3 Anfragerouten 239
7.1.4 Statische Einträge 240
7.1.5 DynDNS 240
7.2 DHCP 243
7.2.1 Server 244
7.2.2 Relay 247
7.2.3 Statische Zuordnungen 248
7.2.4 IPv4-Lease-Tabelle 248
7.2.5 IPv6-Lease-Tabelle 250
7.2.6 Optionen 251
7.3 NTP 254

8 Network Protection 255

8.1 Firewall 255
8.1.1 Regeln 256
8.1.2 Country-Blocking 260
8.1.3 Country-Blocking-Ausnahmen 261
8.1.4 ICMP 262
8.1.5 Erweitert 264
8.2 NAT 266
8.2.1 Maskierung (Masquerading) 267
8.2.2 NAT 268
8.3 Advanced Threat Protection 272
8.3.1 Allgemein 272
8.4 Intrusion Prevention 274
8.4.1 Allgemein 274
8.4.2 Angriffsmuster 275
8.4.3 Anti-DoS/Flooding 276
8.4.4 Anti-Portscan 278
8.4.5 Ausnahmen 280
8.4.6 Erweitert 282
8.5 Server-Lastverteilung 284
8.5.1 Verteilungsregeln 284
8.6 VoIP 287
8.6.1 SIP 287
8.6.2 H.323 289
8.7 Erweitert 290
8.7.1 Generischer Proxy 290

8.7.2 SOCKS-Proxy 291
8.7.3 IDENT-Reverse-Proxy 293

9 Web Protection 295

9.1 Webfilter 296
9.1.1 Webfilter-Änderungen 296
9.1.1.1 Wichtige Unterschiede 297
9.1.1.2 Häufige Aufgaben 297
9.1.1.3 Migration 299
9.1.2 Allgemein 300
9.1.3 Richtlinien 304
9.1.3.1 Filteraktionsassistent 306
9.1.3.2 Kategorien 306
9.1.3.3 Websites 308
9.1.3.4 Downloads 310
9.1.3.5 Antivirus 311
9.1.3.6 Zusätzliche Optionen 312
9.2 Webfilter-Profile 314
9.2.1 Filterprofile 314
9.2.2 Filteraktionen 322
9.2.3 Übergeordnete Proxies 322
9.3 Filteroptionen 323
9.3.1 Ausnahmen 323
9.3.2 Websites 326
9.3.3 Benutzer umgehen 327
9.3.4 Potenziell unerwünschte Anwendungen 328
9.3.5 Kategorien 328
9.3.6 HTTPS-CAs 329
9.3.7 Sonstiges 333
9.4 Richtlinientest 338
9.5 Application Control 339
9.5.1 Netzwerksichtbarkeit 340
9.5.2 Application-Control-Regeln 340
9.5.3 Erweitert 343
9.6 FTP 344
9.6.1 Allgemein 344
9.6.2 Antivirus 345
9.6.3 Ausnahmen 346
9.6.4 Erweitert 347

10 Email Protection 349

10.1 SMTP 349

10.1.1 Allgemein 350
10.1.2 Routing 350
10.1.3 Antivirus 352
10.1.4 Antispam 356
10.1.5 Datenschutz 361
10.1.6 Ausnahmen 363
10.1.7 Relaying 365
10.1.8 Erweitert 366
10.2 SMTP-Profile 370
10.3 POP3 375
10.3.1 Allgemein 376
10.3.2 Antivirus 377
10.3.3 Antispam 378
10.3.4 Ausnahmen 380
10.3.5 Erweitert 381
10.4 Email Encryption 386
10.4.1 Allgemein 389
10.4.2 Optionen 390
10.4.3 Interne Benutzer 392
10.4.4 S/MIME-CAs 394
10.4.5 S/MIME-Zertifikate 395
10.4.6 OpenPGP-Schlüssel 396
10.5 SPX-Verschlüsselung 398
10.5.1 SPX-Konfiguration 399
10.5.2 SPX-Vorlagen 401
10.5.3 SophosOutlook-Add-in 404
10.6 Quarantänebericht 405
10.6.1 Allgemein 406
10.6.2 Ausnahmen 407
10.6.3 Erweitert 409
10.7 Mail-Manager 410
10.7.1 Mail-Manager-Fenster 410
10.7.1.1 SMTP-/POP3-Quarantäne 411
10.7.1.2 SMTP-Spool 412
10.7.1.3 SMTP-Protokoll 414
10.7.2 Allgemein 415
10.7.3 Konfiguration 417
11 Endpoint Protection 419
11.1 Computerverwaltung 421
11.1.1 Allgemein 421

11.1.2 Agent installieren 423
11.1.3 Computer verwalten 423
11.1.4 Gruppen verwalten 424
11.1.5 Erweitert 426
11.2 Antivirus 427
11.2.1 Richtlinien 427
11.2.2 Ausnahmen 429
11.3 Device Control 431
11.3.1 Richtlinien 431
11.3.2 Ausnahmen 432
11.4 Endpoint Web Control 435
11.4.1 Allgemein 435
11.4.2 Erweitert 436
11.4.3 Nicht unterstützte Funktionen 436

12 Wireless Protection 439

12.1 Allgemein 440
12.1.1 Allgemein 440
12.1.2 Erweitert 441
12.2 WLAN-Netzwerke 442
12.3 Access Points 446
12.3.1 Übersicht 447
12.3.2 Gruppierung 452
12.4 Mesh-Netzwerke 453
12.5 WLAN-Clients 456
12.6 Hotspots 456
12.6.1 Allgemein 458
12.6.2 Hotspots 459
12.6.3 Voucher-Definitionen 468
12.6.4 Erweitert 469

13 Webserver Protection 471

13.1 Web Application Firewall 471
13.1.1 Virtuelle Webserver 471
13.1.2 Echte Webserver 475
13.1.3 Firewall-Profile 476
13.1.4 Ausnahmen 483
13.1.5 Site-Path-Routing 484
13.1.6 Erweitert 486
13.2 Umkehrauthentifizierung 487
13.2.1 Profile 487
13.2.2 Formularvorlagen 491

13.3 Zertifikatverwaltung 491
13.3.1 Zertifikate 492
13.3.2 Certificate Authority (Zertifizierungsstelle) 492
13.3.3 Sperrlisten (CRLs) 492
13.3.4 Erweitert 492

14 RED-Verwaltung 493

14.1 Übersicht 494
14.2 Allgemeine Einstellungen 494
14.3 Clientverwaltung 496
14.4 Einrichtungshilfe 506
14.5 Tunnelverwaltung 508

15 Site-to-Site-VPN 511

15.1 Amazon VPC 512
15.1.1 Status 512
15.1.2 Einrichtung 513
15.2 IPsec 515
15.2.1 Verbindungen 518
15.2.2 Entfernte Gateways 520
15.2.3 Richtlinien 523
15.2.4 Lokaler RSA-Schlüssel 527
15.2.5 Erweitert 528
15.2.6 Fehlersuche 530
15.3 SSL 531
15.3.1 Verbindungen 531
15.3.2 Einstellungen 534
15.3.3 Erweitert 535
15.4 Zertifikatverwaltung 536
15.4.1 Zertifikate 536
15.4.2 Certificate Authority (Zertifizierungsstelle) 539
15.4.3 Sperrlisten (CRLs) 540
15.4.4 Erweitert 541

16 Fernzugriff 543

16.1 SSL 544
16.1.1 Profile 544
16.1.2 Einstellungen 546
16.1.3 Erweitert 547
16.2 PPTP 548
16.2.1 Allgemein 548
16.2.2 iOS-Geräte 550

16.2.3 Erweitert 551
16.3 L2TP über IPsec 552
16.3.1 Allgemein 552
16.3.2 iOS-Geräte 556
16.3.3 Fehlersuche 556
16.4 IPsec 557
16.4.1 Verbindungen 560
16.4.2 Richtlinien 562
16.4.3 Erweitert 566
16.4.4 Fehlersuche 568
16.5 HTML5-VPN-Portal 569
16.5.1 Allgemein 570
16.6 Cisco VPN Client 574
16.6.1 Allgemein 574
16.6.2 iOS-Geräte 575
16.6.3 Fehlersuche 576
16.7 Erweitert 577
16.8 Zertifikatverwaltung 577
16.8.1 Zertifikate 578
16.8.2 Certificate Authority (Zertifizierungsstelle) 578
16.8.3 Sperrlisten (CRLs) 578
16.8.4 Erweitert 578
17 Protokolle & Berichte 579
17.1 Protokollansicht 581
17.1.1 Heutige Protokolldateien 581
17.1.2 Archivierte Protokolldateien 581
17.1.3 Protokolldateien durchsuchen 582
17.2 Hardware 582
17.2.1 Täglich 582
17.2.2 Wöchentlich 583
17.2.3 Monatlich 584
17.2.4 Jährlich 584
17.3 Netzwerknutzung 584
17.3.1 Täglich 584
17.3.2 Wöchentlich 585
17.3.3 Monatlich 585
17.3.4 Jährlich 585
17.3.5 Bandbreitennutzung 585
17.4 Network Protection 586
17.4.1 Täglich 587

17.4.2 Wöchentlich 587
17.4.3 Monatlich 587
17.4.4 Jährlich 587
17.4.5 Firewall 588
17.4.6 Advanced Threat Protection 589
17.4.7 IPS 589
17.5 Web Protection 590
17.5.1 Internetnutzung 590
17.5.2 Suchmaschinen 595
17.5.3 Abteilungen 598
17.5.4 Geplante Berichte 599
17.5.5 Application Control 600
17.5.6 Entanonymisierung 601
17.6 Email Protection 601
17.6.1 Nutzungsdiagramme 601
17.6.2 Mail-Nutzung 602
17.6.3 Blockierte Mails 603
17.6.4 Entanonymisierung 603
17.7 Wireless Protection 604
17.7.1 Täglich 604
17.7.2 Wöchentlich 605
17.7.3 Monatlich 605
17.7.4 Jährlich 605
17.8 Fernzugriff 605
17.8.1 Aktivität 605
17.8.2 Sitzung 606
17.9 Webserver Protection 607
17.9.1 Nutzungsdiagramme 607
17.9.2 Details 607
17.10 Gesamtbericht 608
17.10.1 Bericht anzeigen 608
17.10.2 Archivierte Gesamtberichte 608
17.10.3 Konfiguration 608
17.11 Protokolleinstellungen 609
17.11.1 Lokale Protokollierung 609
17.11.2 Remote-Syslog-Server 610
17.11.3 Ausgelagerte Protokollarchive 612
17.12 Berichteinstellungen 614
17.12.1 Einstellungen 614
17.12.2 Ausnahmen 617
17.12.3 Anonymisierung 618

18 Support 621
18.1 Dokumentation 621
18.2 Druckbare Konfiguration 622
18.3 Support kontaktieren 622
18.4 Tools 623
18.4.1 Ping-Prüfung 623
18.4.2 Traceroute 624
18.4.3 DNS-Lookup 624
18.5 Erweitert 625
18.5.1 Prozesse 625
18.5.2 LAN-Verbindungen 625
18.5.3 Routen 625
18.5.4 Schnittstellen 626
18.5.5 Konfigurations-Abbild 626
18.5.6 REF auflösen 626
19 Abmelden 627
20 Benutzerportal 629
20.1 Benutzerportal: Mail-Quarantäne 630
20.2 Benutzerportal: Mail-Protokoll 632
20.3 Benutzerportal: POP3-Konten 633
20.4 Benutzerportal: Absender-Whitelist 633
20.5 Benutzerportal: Absender-Blacklist 634
20.6 Benutzerportal: Hotspots 635
20.7 Benutzerportal: Client-Authentifizierung 638
20.8 Benutzerportal: OTP-Token 638
20.9 Benutzerportal: Fernzugriff 639
20.10 Benutzerportal: HTML5-VPN-Portal 640
20.11 Benutzerportal: Kennwort ändern 642
20.12 Benutzerportal: HTTPS-Proxy 642

1 Installation

Dieses Kapitel enthält Informationen über die Installation und Einrichtung von Sophos UTM in Ihrem Netzwerk.Die Installation von Sophos UTM erfolgt in zwei Schritten: Erstens, die Installation der Software; zweitens, die Konfiguration von grundlegenden Systemeinstellungen.Die Software-Installation wird mithilfe eines konsolengestützten Installationsmenüs durchgeführt.Die interne Konfiguration kann von Ihrem Arbeitsplatzrechner aus über die webbasierte Benutzeroberfläche von Sophos UTM namens WebAdmin erfolgen.Bevor Sie mit der Installation beginnen, überprüfen Sie bitte, ob Ihre Hardware den Mindestanforderungen entspricht.

Hinweis – Wenn Sie eine Sophos UTM-Appliance betreiben, können Sie die folgenden Abschnitte überspringen und direkt mit dem Abschnitt *Grundkonfiguration* fortfahren, da bei allen Sophos UTM-Hardware-Appliances die UTM-Software vorinstalliert ist.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Empfohlene Lektüre
- Systemanforderungen
- Installationsanleitung
- Grundkonfiguration
- Backup-Wiederherstellung

1.1 Empfohlene Lektüre

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Dokumente lesen, die Ihnen bei der Einrichtung von Sophos UTM helfen. Beide Dokumente sind der Sophos UTM Hardware Appliance beigelegt und können alternativ vom Sophos UTM-Resource-Center heruntergeladen werden:

- Quick Start Guides Hardware
- Operating Instructions

1.2 Systemanforderungen

Für die Installation und den Betrieb der UTM gelten die folgenden Hardware-Mindestanforderungen:

- **Prozessor:** Pentium 4 mit 1,5 GHz (oder vergleichbar)
- **Speicher:** 1 GB RAM
- **Festplatte:** 20-GB-IDE- oder -SCSI-Festplatte
- **CD-ROM-Laufwerk:** Bootfähiges IDE- oder SCSI-CD-ROM-Laufwerk
- **Netzwerkkarten (NICs):** Zwei oder mehr PCI-Ethernet-Netzwerkkarten
- **Netzwerkkarte** (optional): Eine Heartbeat-fähige PCI-Ethernet-Netzwerkkarte.In einem hochverfügbaren System (HA) kommunizieren das Primärsystem und das Standby-System mittels eines sogenannten Heartbeats miteinander – ein Signal, das über eine Netzwerkverbindung zwischen beiden Systemen zyklisch ausgetauscht wird. Falls Sie ein hochverfügbares System einsetzen möchten, stellen Sie sicher, dass beide Geräte mit Heartbeat-fähigen Netzwerkkarten ausgestattet sind.
- **USB** (optional): Ein USB-Anschluss zur Kommunikation mit einem USV-Gerät
- **Switch** (optional): Ein Gerät, das die Kommunikation in Computernetzwerken steuert. Stellen Sie sicher, dass der Switch sogenannte Jumbo Frames unterstützt.

Sophosführt eine Liste aller Hardware-Produkte, die im Zusammenhang mit der UTM-Software auf ihre Funktionalität hin getestet wurden.Die *Hardwarekompatibilitätsliste (Hardware Compatibility List*; HCL) steht in SophosKnowledgebase zur Verfügung.Um Installations- und Betriebsfehler mit der UTM-Software zu vermeiden, sollten Sie nur Hardware verwenden, die in der HCL aufgeführt ist. Die Hardware- und Software-Anforderungen an den Arbeitsplatzrechner für den Zugriff auf die webbasierte Benutzeroberfläche WebAdmin sind wie folgt:

- **Prozessor:** Taktfrequenz 1 GHz oder höher
- **Browser:** Neuste Version von Firefox (empfohlen), neuste Version von Chrome, neuste Version von Safari, oder Microsoft Internet Explorer 8 und höher. JavaScript muss aktiviert sein.Darüber hinaus darf im Browser kein Proxy für die IP-Adresse der internen Netzwerkkarte (eth0) von UTM konfiguriert sein.

1.2.1 USV-Unterstützung

Geräte zur unterbrechungsfreien Stromversorgung (USV) gewährleisten eine kontinuierliche Stromversorgung bei Störungen oder Schwankungen der Stromzufuhr, indem sie Strom aus einer unabhängigen Stromquelle liefern, wenn der Hausstrom ausfällt.Sophos UTMunterstützt Geräte der Hersteller MGE UPS Systems und APC.Die Kommunikation zwischen dem USV-Gerät und Sophos UTM erfolgt über die USB-Schnittstelle.

Sobald das USV-Gerät im Batteriebetrieb läuft, wird eine Nachricht an den Administrator geschickt.Falls die Stromunterbrechung für einen längeren Zeitraum andauert und der Batteriestatus des USV-Geräts einen kritischen Wert erreicht, wird eine weitere Nachricht verschickt. Sophos UTM fährt anschließend kontrolliert herunter und schaltet sich automatisch ab.

Hinweis – Informationen darüber, wie Sie Sophos UTM an Ihrem USV-Gerät anschließen können, finden Sie in der Bedienungsanleitung des USV-Geräts.UTMerkennt das an der USB-Schnittstelle angeschlossene USV-Gerät während des Systemstarts.Starten Sie Sophos UTM daher erst nach der Verbindung mit dem USV-Gerät.

1.2.2 RAID-Unterstützung

Ein RAID-System (*Redundant Array of Independent Disks*) ist ein Datenspeicherungsschema mit mehreren Festplatten, die gemeinsam auf Daten zugreifen oder diese replizieren.Um sicherzustellen, dass das RAID-System erkannt und korrekt auf dem Dashboard des WebAdmin angezeigt wird, benötigen Sie einen RAID-Controller, der von Sophos UTM unterstützt wird.Auf der HCL) können Sie nachsehen, welche RAID-Controller unterstützt werden.Die HCL befindet sich in der SophosKnowledgebase. Verwenden Sie „HCL“ als Suchbegriff, um die entsprechende Seite zu finden.

1.3 Installationsanleitung

Im Folgenden wird die Installation der Sophos UTM-Software Schritt für Schritt beschrieben.

Bevor Sie mit der Installation beginnen, halten Sie die folgenden Komponenten bereit:

- Die Sophos UTM CD-ROM
- die Lizenz fürSophos UTM

Das Installationsprogramm überprüft zunächst die Hardware und installiert dann die Software auf Ihrem System.

1.3.1 Tastenfunktionen während der Installation

Die Navigation im Installationsmenü erfolgt über die folgenden Tasten (beachten Sie während der Installation auch die zusätzlichen Tastenfunktionen, die unten im Bild angezeigt werden):

- F1: Zeigt den kontextsensitiven Hilfebildschirm an.
- Pfeiltasten: Navigation in den Textfeldern, z. B. in der Lizenzbestimmung und der Auswahl des Tastatur-Layouts.
- Tabulatortaste: Wechseln zwischen den Textfeldern, Listen und Schaltflächen.
- Eingabetaste: Die Eingabe wird bestätigt und die Installation wird mit dem nächsten Schritt fortgesetzt.
- Leertaste: Wählen Sie Optionen, die mit einem Asterisk markiert sind, aus oder ab.
- Alt-F2: Wechsel zur Installationskonsole.
- Alt-F4: Wechsel zum Protokoll.
- Alt-F1: Wechsel zur interaktiven Bash-Konsole.
- Alt-F1: Rückkehr zum Haupt-Installationsbildschirm.

1.3.2 Besondere Optionen während der Installation

Einige Installationsschritte bieten zusätzliche Optionen an:

View Log: Anzeige des Installationsprotokolls.

Support: Anzeige des Dialogfensters für Unterstützung.

To USB Stick: Speichern des Installationsprotokolls als zip-Datei auf einen USB-Stick. Denken Sie daran, einen USB-Stick einzustecken, bevor Sie diese Option bestätigen.Die zip-Datei kann dazu verwendet werden, Installationsprobleme zu lösen, z. B. durch das Support-Team von Sophos UTM.

Back: Rückkehr zum letzten Installationsschritt.

Cancel: Anzeige eines Bestätigungsdialogfensters, um die Installation abzubrechen.

Help: Anzeige des kontextsensitiven Hilfebildschirms.

1.3.3 Installation vonSophos UTM

1. **Booten Sie den PC von der CD-ROM.**
   Der Startbildschirm der Installation wird angezeigt.

   Hinweis – Sie können jederzeit F1 drücken, um zum Hilfebildschirm zu gelangen. Durch Drücken von F3 im Startbildschirm wird ein Bildschirm zur Fehlerbehebung angezeigt.

2. **Drücken Sie die Eingabetaste.**
   Der Schritt *Introduction* (Einleitung) wird angezeigt.

3. **Wählen Sie *Start Installation* (Installation starten).**
   Der Schritt *Hardware Detection* (Hardware-Erkennung) wird angezeigt.

   Die Software prüft die folgenden Hardware-Komponenten:

   - Prozessor
   - Größe und Fabrikat der Festplatte
   - CD-ROM-Laufwerk
   - Netzwerkkarten
   - IDE- bzw. SCSI-Controller

   Falls Ihr System die Mindestvoraussetzungen nicht erfüllt, wird die Installation mit einer entsprechenden Fehlermeldung abgebrochen.

   Sobald die Hardware-Erkennung abgeschlossen ist, wird der Schritt *Detected Hardware* (Erkannte Hardware) zu Informationszwecken angezeigt.

4. **Drücken Sie die Eingabetaste.**
   Der Schritt *Select Keyboard* (Tastatur-Layout wählen) wird angezeigt.

5. **Wählen Sie Ihr Tastatur-Layout.**
   Wählen Sie mit den Pfeiltasten das Tastatur-Layout aus, z. B. *German (DE)*, und bestätigen Sie dies mit der Eingabetaste.

   Der Schritt *Select Timezone* (Zeitzone wählen) wird angezeigt.

6. **Wählen Sie Ihre Region.**
   Wählen Sie mit den Pfeiltasten Ihre Region aus, z. B. *Europe* (Europa), und bestätigen Sie dies mit der Eingabetaste.

7. **Wählen Sie Ihre Zeitzone.**
   Wählen Sie mit den Pfeiltasten Ihre Zeitzone aus, z. B. *Berlin*, und bestätigen Sie dies mit der Eingabetaste.

   Der Schritt *Date and Time* (Datum und Zeit) wird angezeigt.

8. **Stellen Sie Datum und Uhrzeit ein.**
   Falls Datum und Zeit nicht korrekt sind, können Sie die Einstellungen hier ändern. Sie können mit der Tabulator-Taste und den Pfeiltasten zwischen den Textfeldern wechseln.Mit der Leertaste können Sie die Option *Host Clock is UTC* (Systemuhr ist UTC) abwählen. Ungültige Eingaben werden nicht übernommen. Bestätigen Sie die Eingaben mit der Eingabetaste.

   Der Schritt *Select Admin Interface* (Administrationsschnittstelle wählen) wird angezeigt.

9. **Wählen Sie eine interne Netzwerkkarte.**
   Damit Sie nach der Installation Sophos UTM über die Benutzeroberfläche WebAdmin weiter konfigurieren können, müssen Sie eine Netzwerkkarte als interne Netzwerkschnittstelle (eth0) definieren. Wählen Sie aus der verfügbaren Hardware eine Netzwerkkarte aus und bestätigen Sie die Auswahl mit der Eingabetaste.

   Hinweis – Schnittstellen, die eine aktive Verbindung haben, sind mit dem Wort *[Link]* hervorgehoben.

   Der Schritt *Network Configuration* (Netzwerkkonfiguration) wird angezeigt.

10. **Konfigurieren Sie die Netzwerkschnittstelle für die Administration.**
    Definieren Sie für die interne Schnittstelle, über die das System administriert werden soll, eine IP-Adresse, eine Netzmaske und ein Standardgateway. Die Standardwerte sind:

    Adresse: `192.168.2.100`

    Netzmaske: `255.255.255.0`

    Gateway: `–`

    Den Wert für das Standardgateway müssen Sie nur ändern, wenn Sie die WebAdmin-Schnittstelle von einem PC aus erreichen möchten, der außerhalb des

Netzwerkbereichs liegt.Beachten Sie, dass sich das Gateway innerhalb des Subnetzes befinden muss.[1]

Bestätigen Sie die Eingaben mit der Eingabetaste.

Wenn Ihr Prozessor 64 Bit unterstützt, wird der Schritt *64 Bit Kernel Support* (64-Bit-Kernel-Unterstützung) angezeigt.Andernfalls wird die Installation mit dem Schritt *Enterprise Toolkit* fortgesetzt.

11. **Installieren Sie den 64-Bit-Kernel.**
Wählen Sie *Yes*, um den 64-Bit-Kernel zu installieren, oder *No*, um den 32-Bit-Kernel zu installieren.

    Der Schritt *Enterprise Toolkit* wird angezeigt.

12. **Akzeptieren Sie die Installation des Enterprise Toolkits.**
Das Enterprise Toolkit umfasst die Sophos UTM-Software.Sie können beschließen, nur Open-Source-Software zu installieren.Wir empfehlen jedoch auch die Installation des Enterprise Toolkits, sodass Sie die volle Funktionalität von Sophos UTM verwenden können.

    Drücken Sie die Eingabetaste, um beide Softwarepakete zu installieren, oder wählen Sie *No*, um nur die Open-Source-Software zu installieren.

    Der Schritt *Installation: Partitioning* (Installation: Partitionierung) wird angezeigt.

13. **Bestätigen Sie den Warnhinweis, um die Installation zu starten.**
Bitte lesen Sie den Warnhinweis sorgfältig.Nach der Bestätigung werden alle bestehenden Daten auf dem PC gelöscht.

    Wenn Sie die Installation abbrechen und das System stattdessen neu starten möchten, wählen Sie *No*.

    Warnung – Alle Daten auf der Festplatte werden gelöscht.

---

[1]Bei der Netzmaske `255.255.255.0` wird das Subnetz durch die ersten drei Werte definiert. In unserem Beispiel lautet der relevante Bereich `192.168.2`.Wenn nun Ihr Administrations-PC z. B. die IP-Adresse `192.168.10.5` hat, liegt er nicht im selben Subnetz. In diesem Fall benötigen Sie ein Gateway.Das Gateway muss dann eine Schnittstelle im `192.168.2`-Subnetz und eine Verbindung zum Administrations-PC haben.Für unser Beispiel nehmen wir die Adresse `192.168.2.1`.

Die Installation der Software kann nun einige Minuten dauern.

Der Schritt *Installation Finished* (Installation abgeschlossen) wird angezeigt.

14. **Entnehmen Sie die CD-ROM, verbinden Sie das System mit dem internen Netzwerk und starten Sie das System neu.**
Sobald Sie dazu aufgefordert werden, entnehmen Sie die CD-ROM aus dem Laufwerk und verbinden die Netzwerkkarte `eth0` mit Ihrem lokalen Netzwerk.Mit Ausnahme der internen Netzwerkkarte (`eth0`) wird die Reihenfolge der Netzwerkkarten in erster Linie durch die PCI-ID und die Kernel-Treiber bestimmt. Die Reihenfolge der Netzwerkkartenbenennung kann sich auch später durch Änderung der Hardwarekonfiguration, z. B. durch das Hinzufügen oder Entfernen von Netzwerkkarten, ändern.

    Drücken Sie im Installationsmenü dann die Eingabetaste, um UTM neu zu starten. Während des Neustarts werden die IP-Adressen der internen Netzwerkkarten neu gesetzt, daher kann auf der Installationsroutine-Konsole (Alt+F1) für kurze Zeit die Meldung „No IP on eth0” stehen.

Nachdem Sophos UTM neu gestartet ist (je nach Hardware-Leistung kann dies einige Minuten dauern), sollten Sie mit dem Programm Ping die IP-Adresse der internen Netzwerkkarte `eth0` erreichen. Falls keine Verbindung zustande kommt, prüfen Sie Ihr System auf die nachfolgenden möglichen Fehlerquellen:

- Die IP-Adresse von Sophos UTM ist nicht korrekt gesetzt.
- Die IP-Adresse des Administrations-PCs ist nicht korrekt gesetzt.
- Das Standardgateway ist nicht korrekt gesetzt.
- Das Netzwerkkabel ist mit der falschen Netzwerkkarte verbunden.
- Alle Netzwerkkarten sind an einem Hub angeschlossen.

1.4 Grundkonfiguration

Der zweite Teil der Installation erfolgt im WebAdmin, der webbasierten Administrator-Benutzeroberfläche von Sophos UTM.Bevor Sie die Grundkonfiguration durchführen, sollten Sie eine Vorstellung davon haben, wie Sie die Sophos UTM in Ihr Netzwerk integrieren wollen. Sie müssen entscheiden, welche Funktionen sie bereitstellen soll, z. B., ob sie im Bridge-Modus oder im Standard-Modus (Routing) arbeiten soll, oder ob sie den Datenpaketfluss zwischen ihren Schnittstellen überwachen soll.Sie können die Sophos UTM jedoch immer zu einem

späteren Zeitpunkt neu konfigurieren. Wenn Sie also noch nicht geplant haben, wie Sie die Sophos UTM in Ihr Netzwerk integrieren wollen, können Sie direkt mit der Grundkonfiguration beginnen.

1. **Starten Sie Ihren Browser und öffnen Sie den WebAdmin.**
   Rufen Sie die URL der Sophos UTM auf (d. h. die IP-Adresse von eth0).Um bei unserer Beispielkonfiguration zu bleiben, ist dies die URL `https://192.168.2.100:4444` (beachten Sie das HTTPS-Protokoll und die Portnummer 4444).

   Beachten Sie, dass abweichend von der betrachteten Beispielkonfiguration jede Sophos UTM mit den folgenden Standardeinstellungen ausgeliefert wird:

   - **Schnittstellen:** Interne Netzwerkschnittstelle (eth0)
   - **IP-Adresse:** 192.168.0.1
   - **Netzmaske:** 255.255.255.0
   - **Standardgateway:** –

   Um auf den WebAdmin einer beliebigen Sophos UTM zuzugreifen, geben Sie stattdessen folgende URL an:

   `https://192.168.0.1:4444`

   Um Authentifizierung und verschlüsselte Kommunikation zu gewährleisten, wird die Sophos UTM mit einem selbstsignierten Sicherheitszertifikat ausgeliefert. Dieses Zertifikat wird dem Webbrowser beim Aufbau der HTTPS-basierten Verbindung zum WebAdmin angeboten. Da er die Gültigkeit des Zertifikats nicht überprüfen kann, zeigt der Browser eine Sicherheitswarnung an. Nachdem Sie das Zertifikat akzeptiert haben, wird die initiale Anmeldeseite angezeigt.

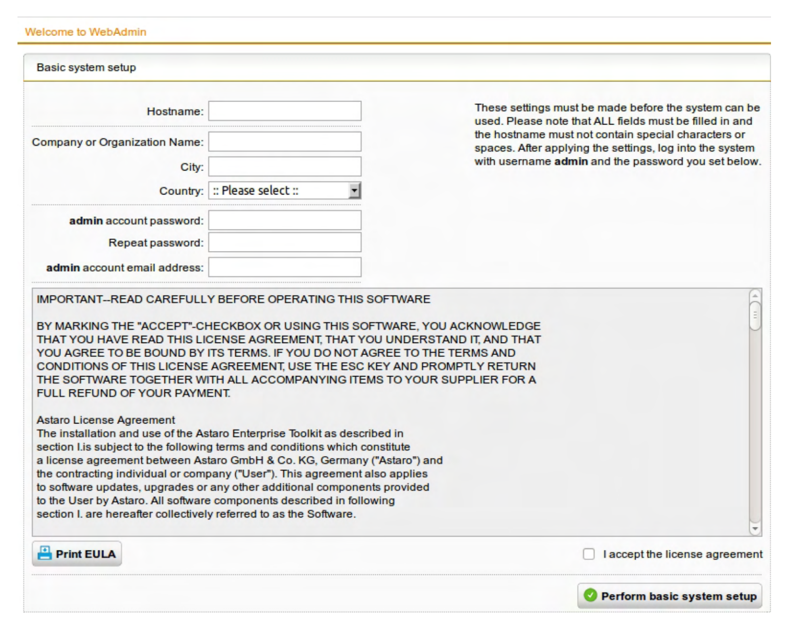


Bild 1 WebAdmin: Initiale Anmeldeseite

2. **Füllen Sie das Anmeldeformular aus.**
   Geben Sie die genauen Informationen zu Ihrer Firma in die Textfelder ein.Legen Sie ein Kennwort fest und geben Sie eine gültige E-Mail-Adresse für das Administratorkonto ein. Wenn Sie mit den Lizenzbestimmungen einverstanden sind, klicken Sie auf die Schaltfläche *Grundlegende Systemkonfiguration durchführen*, um mit dem Anmeldevorgang fortzufahren. Während dieses Vorganges werden einige digitale Zertifikate und CAs (Certificate Authorities, dt. Zertifizierungsstellen) erzeugt:

   - **WebAdmin CA:** Die CA, mit der das WebAdmin-Zertifikat signiert wurde (siehe *Verwaltung > WebAdmin-Einstellungen > HTTPS-Zertifikat*).
   - **VPN-Signierungs-CA:** Die CA, mit der digitale Zertifikate für VPN-Verbindungen signiert werden (siehe *Site-to-Site-VPN > Zertifikatverwaltung > Zertifizierungsstelle*).
   - **WebAdmin-Zertifikat:** Das digitale Zertifikat von WebAdmin (siehe *Site-to-Site-VPN > Zertifikatverwaltung > Zertifikate*).

- **Lokales X.509-Zertifikat:** Das digitale Zertifikat von Sophos UTM wird für VPN-Verbindungen verwendet (siehe *Site-to-Site VPN* > *Zertifikatverwaltung* > *Zertifikate*).

Die Anmeldeseite wird angezeigt.(Bei einigen Browsern kann es passieren, dass Ihnen ein weiterer Sicherheitshinweis angezeigt wird, weil sich das Zertifikat entsprechend Ihren Eingaben geändert hat.)

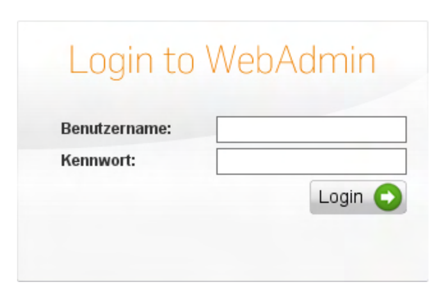


Bild 2 WebAdmin: Reguläre Anmeldeseite

3. **Melden Sie sich am WebAdmin an.**
   Geben Sie in das Feld *Benutzername* das Wort `admin` ein und geben Sie das Kennwort ein, das Sie in der vorherigen Ansicht festgelegt haben.

   Ihnen wird nun ein Konfigurationsassistent angezeigt, der Sie durch den ersten Konfigurationsprozess leitet.

   Fortfahren: Wenn Sie den Assistenten verwenden möchten, wählen Sie diese Option und klicken Sie auf *Weiter*.Führen Sie die Schritte aus, um die Grundeinstellungen der Sophos UTM zu konfigurieren.

   Ein Backup wiederherstellen: Falls Sie über eine Backupdatei verfügen, können Sie stattdessen auch das Backup wiederherstellen. Wählen Sie diese Option und klicken Sie auf *Weiter*.Wie Sie fortfahren, ist in Abschnitt *Backup-Wiederherstellung* beschrieben.

   Alternativ können Sie auch bedenkenlos auf *Abbrechen* klicken (in jedem der Schritte des Assistenten) und dadurch den Assistenten beenden, wenn Sie z. B. die Konfiguration der Sophos UTM direkt im WebAdmin vornehmen möchten. Sie können auch jederzeit auf *Fertigstellen* klicken. Dann werden alle bis dahin vorgenommenen Einstellungen gespeichert und der Assistent beendet.

4. **Installieren Sie Ihre Lizenz.**
   Klicken Sie auf das Ordnersymbol, um Ihre erworbene Lizenz (eine Textdatei) hochzuladen. Klicken Sie auf *Weiter*, um die Lizenz zu installieren. Falls Sie keine Lizenz erworben haben, klicken Sie auf *Weiter*, um die 30-Tage-Evaluationslizenz zu verwenden, bei der alle Produktmerkmale aktiviert sind und die mit der Sophos UTM ausgeliefert werden.

   > **Hinweis –** Wenn die ausgewählte Lizenz ein bestimmtes Abonnement nicht enthält, wird die entsprechende Seite im weiteren Verlauf deaktiviert.

5. **Konfigurieren Sie die interne Netzwerkkarte.**
   Überprüfen Sie die angezeigten Einstellungen für die interne Netzwerkschnittstelle (*eth0*). Die vorliegenden Einstellungen resultieren aus den Informationen, die Sie während der Installation der Software eingegeben haben. Zusätzlich können Sie die Sophos UTM als DHCP-Server auf der internen Schnittstelle konfigurieren, indem Sie das entsprechende Auswahlkästchen markieren.

   > **Hinweis –** Wenn Sie die IP-Adresse der internen Netzwerkschnittstelle ändern, müssen Sie sich mit der neuen IP-Adresse erneut am WebAdmin anmelden, wenn Sie den Assistenten beendet haben.

6. **Wählen Sie den Uplink-Typ für die externe Netzwerkkarte.**
   Wählen Sie die Art der Verbindung Ihrer Uplink-/Internetverbindung, die die externe Netzwerkkarte verwenden wird. Die Art der Schnittstelle und ihre Konfiguration hängen davon ab, welche Art der Internetverbindung Sie verwenden werden.Klicken Sie auf *Weiter*.

   Falls die Sophos UTM über keinen Uplink verfügt oder Sie diesen jetzt noch nicht konfigurieren möchten, wählen Sie die Option *Internetverbindung später einrichten*. Wenn Sie einen Internet-Uplink konfigurieren, wird IP-Maskierung automatisch für alle Verbindungen aus dem internen Netzwerk zum Internet konfiguriert.

   Wenn Sie *Standard-Ethernetschnittstelle mit statischer IP-Adresse* auswählen, ist ein *Standardgateway* nur optional anzugeben. Wenn Sie das Textfeld leer lassen, bleibt Ihre -Standardgateway-Einstellung aus der Installationsroutine erhalten. Sie können jeden der folgenden Schritte überspringen, indem Sie auf *Weiter* klicken. Diese übergangenen Einstellungen können Sie dann später im WebAdmin vornehmen oder ändern.

> **Hinweis –** Wenn Ihre Lizenz keine der folgenden Funktionen unterstützt, wird die entsprechende Funktion nicht angezeigt.

7. **Legen Sie die grundlegenden Firewall-Einstellungen fest.**
   Hier können Sie auswählen, welche Arten von Diensten Sie für das Internet zulassen wollen. Klicken Sie auf *Weiter*, um Ihre Einstellungen zu bestätigen.
8. **Legen Sie die Advanced-Threat-Protection-Einstellungen fest.**
   Hier können Sie Einstellungen festlegen, die den Angriffschutz und Command & Control/Botnet-Erkennung für verschiedene Betriebssysteme und Datenbanken betreffen. Klicken Sie auf *Weiter*, um Ihre Einstellungen zu bestätigen.
9. **Legen Sie die Web-Protection-Einstellungen fest.**
   Hier können Sie festlegen, ob Internetverkehr nach Viren und Spionagesoftware (Spyware) gescannt werden soll. Darüber hinaus können Sie Websites bestimmter Kategorien blockieren lassen. Klicken Sie auf *Weiter*, um Ihre Einstellungen zu bestätigen.
10. **Legen Sie die Email-Protection-Einstellungen fest.**
    Hier können Sie das erste Auswahlkästchen markieren, um den POP3-Proxy zu aktivieren. Wenn Sie das zweite Auswahlkästchen markieren, fungiert die UTM als SMTP-Relay für eingehende Mails: Geben Sie die IP-Adresse Ihres internen Mailservers an und fügen Sie SMTP-Domänen hinzu, die geroutet werden sollen. Klicken Sie auf *Weiter*, um Ihre Einstellungen zu bestätigen.
11. **Legen Sie die Wireless-Protection-Einstellungen fest.**
    Hier können Sie das Auswahlkästchen markieren, um Wireless Protection zu aktivieren. Wählen Sie im Feld die Schnittstellen aus, die Ihre Wireless Access Points mit Ihrem System verbinden dürfen, oder fügen Sie sie hinzu. Klicken Sie auf das Ordnersymbol, um eine Schnittstelle hinzuzufügen, oder klicken Sie auf das Plussymbol, um eine neue Schnittstelle zu erstellen. Geben Sie die anderen Parameter für das WLAN-Netzwerk ein.Klicken Sie auf *Weiter*, um Ihre Einstellungen zu bestätigen.
12. **Legen Sie die Advanced-Threat-Adaptive-Learning-Einstellungen fest.**
    Nun haben Sie die Wahl, anonyme Daten an das Forschungsteam von Sophos zu senden. Diese Daten werden genutzt, um zukünftige Versionen zu verbessern und die Netzwerksichtbarkeits- und Application-Control-Bibliothek zu verbessern und zu erweitern.
13. **Bestätigen Sie Ihre Einstellungen.**

Es wird Ihnen eine Aufstellung der vorgenommenen Einstellungen angezeigt.Klicken Sie auf *Fertigstellen*, um sie zu bestätigen, oder auf *Zurück*, um sie zu ändern. Sie können die Einstellungen jedoch auch später im WebAdmin ändern.

Nachdem Sie auf *Fertigstellen* geklickt haben, wird das Dashboard des WebAdmin angezeigt, das Sie auf einen Blick über den aktuellen Systemstatus der Sophos UTM informiert.

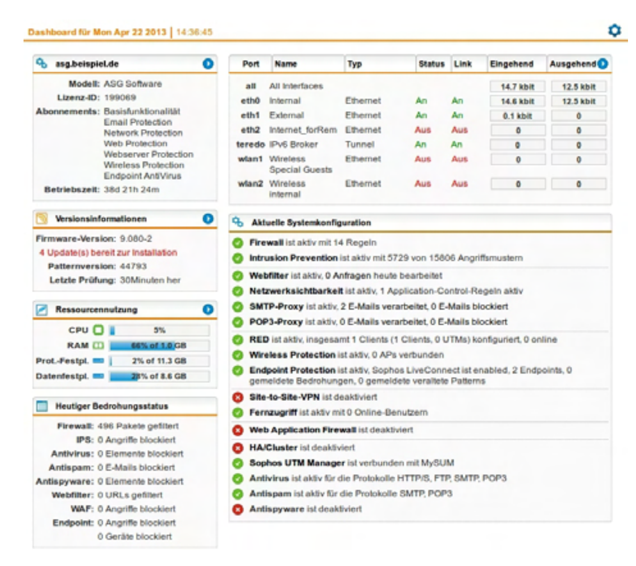


Bild 3 WebAdmin: Dashboard

Falls Sie bei einzelnen Schritten des Assistenten auf Probleme stoßen, wenden Sie sich bitte an die Support-Abteilung Ihres Sophos UTM-Anbieters. Weitergehende Informationen finden Sie auf den folgenden Webseiten:

- Sophos UTMSupport-Forum
- SophosKnowledgebase

1.5 Backup-Wiederherstellung

Der Konfigurationsassistent des WebAdmin (siehe Abschnitt *Grundkonfiguration*) ermöglicht es Ihnen, eine vorhandene Backupdatei wiederherzustellen, anstatt die Grundkonfiguration durchzuführen. Gehen Sie folgendermaßen vor:

1. **Wählen Sie im Konfigurationsassistenten *Vorhandene Backup-Datei wiederherstellen*.**
   Wählen Sie im Konfigurationsassistenten *Vorhandene Backup-Datei wiederherstellen* und klicken Sie auf *Weiter*.

   Sie werden zu der Seite weitergeleitet, auf der Sie die Datei hochladen können.

2. **Laden Sie das Backup hoch**.
   Klicken Sie auf das Ordnersymbol, wählen Sie die Backupdatei aus, die Sie wiederherstellen möchten, und klicken Sie auf *Hochladen starten*.

3. **Stellen Sie das Backup wieder her**.
   Klicken Sie auf *Fertigstellen*, um das Backup wiederherzustellen.

Wichtiger Hinweis – Danach ist es nicht mehr möglich, den Konfigurationsassistenten erneut aufzurufen.

Sobald das Backup erfolgreich wiederhergestellt wurde, werden Sie auf die Anmeldeseite weitergeleitet.

2 WebAdmin

Der WebAdmin ist die webbasierte grafische Benutzeroberfläche zur vollständigen Administration von Sophos UTM. Der WebAdmin besteht aus einem Menü und mehreren Seiten, von denen manche wiederum mehrere Registerkarten (engl. tabs) besitzen. Das Menü auf der linken Seite orientiert sich in logischer Reihenfolge an den Produktmerkmalen von Sophos UTM. Sobald Sie auf einen Menüpunkt wie z. B. *Network Protection* klicken, öffnet sich ein Untermenü und die entsprechende Seite wird angezeigt. Beachten Sie, dass für einige Menüpunkte keine eigene Seite vorhanden ist. In diesem Fall wird weiterhin die zuvor ausgewählte Seite angezeigt. Erst wenn Sie ein Untermenü anklicken, öffnet sich die dazugehörige Seite, und zwar mit der ersten Registerkarte.

Die Anleitungen in dieser Dokumentation führen Sie durch die Angabe des Menüs, Untermenüs und der Registerkarte zu einer Seite, z. B.: „Auf der Registerkarte *Schnittstellen & Routing > Schnittstellen > Hardware* werden ...“

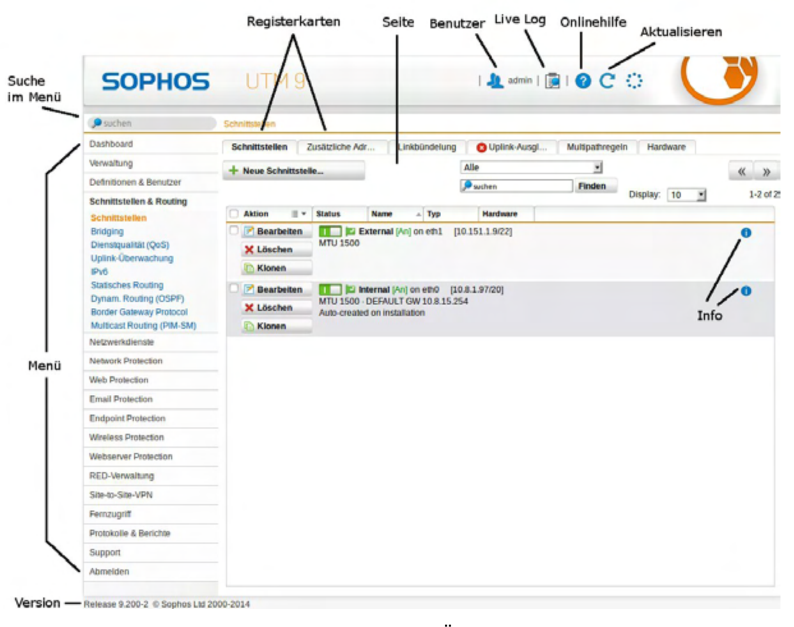


Bild 4 WebAdmin: Übersicht

2.1 WebAdmin-Menü

Das WebAdmin-Menü gibt Ihnen Zugriff auf alle Konfigurationsoptionen von Sophos UTM. Die Verwendung einer Kommandozeile zur Konfiguration ist daher nicht erforderlich.

- **Dashboard:** Das Dashboard zeigt eine grafische Momentaufnahme des Betriebsstatus von Sophos UTM.
- **Verwaltung:** In diesem Menü werden grundlegende Einstellungen für das Gesamtsystem und WebAdmin vorgenommen, sowie Einstellungen, welche die Konfiguration von Sophos UTM betreffen.
- **Definitionen & Benutzer:** Neben Netzwerk-, Dienst- und Zeitereignisdefinitionen sowie Benutzerkonten und -gruppen werden in diesem Menü externe Authentifizierungsdienste für Sophos UTM konfiguriert.
- **Schnittstellen & Routing:** Dieses Menü enthält u. a. die Konfiguration von Netzwerkschnittstellen und Routing-Optionen.
- **Netzwerkdienste:** Dieses Menü enthält u. a. die Konfiguration von Netzwerkdiensten wie DNS und DHCP.
- **Network Protection:** Konfiguration von grundlegenden Network Protection-Funktionen wie Firewall-Regeln, Voice over IP oder Einstellungen für das Angriffschutzsystem.
- **Web Protection:** Konfiguration des Webfilters und von Application Control von Sophos UTM sowie des FTP-Proxys.
- **Email Protection:** Konfiguration der SMTP- und POP3-Proxies von Sophos UTM sowie der E-Mail-Verschlüsselung.
- **Endpoint Protection:** Konfiguration und Verwaltung des Schutzes von Endpoint-Geräten in Ihrem Netzwerk.
- **Wireless Protection:** Konfiguration Ihrer Drahtlosnetzwerke für das Gateway.
- **Webserver Protection:** Zum Schutz Ihrer Webserver vor Angriffen wie Cross-Site-Scripting und SQL-Injection.
- **RED-Verwaltung:** Konfiguration Ihrer RED-Appliances (Remote Ethernet Device).
- **Site-to-Site-VPN:** Konfiguration von Site-to-Site-Virtual-Private-Networks.
- **Fernzugriff:** Konfiguration von VPN-Fernzugriffsverbindungen mit Sophos UTM.

- **Protokolle & Berichte:** Anzeige von Protokollen und Statistiken zur Nutzung von Sophos UTM und Konfiguration von Protokoll- und Berichteinstellungen.
- **Support:** Hier finden Sie verschiedene Support-Tools von Sophos UTM.
- **Log Off:** Abmelden von der Benutzeroberfläche.

Suche im Menü

Über dem Menü befindet sich ein Suchfeld. Damit können Sie das Menü nach Stichwörtern durchsuchen, um so leichter Menüeinträge zu finden, die ein bestimmtes Thema betreffen. Die Suchfunktion berücksichtigt neben den Namen von Menüeinträgen auch hinterlegte, indizierte Aliasse und Schlüsselwörter.

Sobald Sie anfangen im Suchfeld zu tippen, wird das Menü automatisch auf relevante Menüeinträge reduziert. Sie können das Suchfeld jederzeit verlassen und auf den Menüeintrag klicken, der dem Gesuchten entspricht. Das reduzierte Menü bleibt erhalten und zeigt die Suchergebnisse solange an, bis Sie es über die Schaltfläche direkt daneben zurücksetzen.

Tipp – Sie können den Fokus auf das Suchfeld setzen, indem Sie auf der Tastatur `STRG+Y` drücken.

2.2 Symbolleiste

Die Symbole in der oberen rechten Ecke des WebAdmin bieten Zugriff auf die folgenden Funktionen:

- **Benutzername/IP:** Zeigt den aktuell angemeldeten Benutzer und die IP-Adresse an, von der aus auf WebAdmin zugegriffen wird. Wenn derzeit noch weitere Benutzer angemeldet sind, werden ihre Daten ebenfalls angezeigt.
- **Live-Protokoll öffnen:** Wenn Sie diese Schaltfläche anklicken, wird das Live-Protokoll, das dem aktiven WebAdmin-Menü oder der aktiven Registerkarte zugeordnet ist, geöffnet. Um ein anderes Live-Protokoll aufzurufen, ohne in ein anderes Menü oder auf eine andere Registerkarte zu wechseln, fahren Sie mit dem Mauszeiger über die Schaltfläche „Live-Protokoll“. Nach ein paar Sekunden wird eine Liste der verfügbaren Live-Protokolle geöffnet, aus der Sie das anzuzeigende Live-Protokoll auswählen können. Ihre Auswahl wird so lange beibehalten, wie Sie sich im gleichen Menü bzw. auf der gleichen Registerkarte des WebAdmin befinden.

> **Tipp –** Sie können Live-Protokolle auch über die Schaltflächen *Live-Protokoll öffnen* öffnen, die Sie auf vielen WebAdmin-Seiten finden.

- **Onlinehilfe:** Jedes Menü, Untermenü und jede Registerkarte verfügt über eine kontextsensitive Onlinehilfe, die Informationen und Anleitungen zu der jeweils geöffneten Seite von WebAdmin enthält.

> **Hinweis –** Die Onlinehilfe ist versionsbasiert und wird mithilfe von Patterns aktualisiert. Wenn Sie eine Aktualisierung auf eine neue Firmware-Version durchführen, wird auch Ihre Onlinehilfe gegebenenfalls aktualisiert.

- **Aktualisieren:** Klicken Sie stets auf die Schaltfläche *Aktualisieren*, um die bereits angezeigte Seite von WebAdmin zu aktualisieren.

> **Hinweis –** Verwenden Sie nie die Aktualisierungsfunktion des Browsers, da Sie in diesem Fall vom WebAdmin abgemeldet werden.

2.3 Listen

Viele Seiten im WebAdmin bestehen aus Listen.Mit den Schaltflächen links von jedem Listeneintrag können Sie einen Listeneintrag bearbeiten, löschen oder klonen (weitere Informationen finden Sie im Abschnitt *Schaltflächen und Symbole*). Zum Erstellen eines neuen Listeneintrags klicken Sie auf die Schaltfläche *Neue …* (wobei „…“ als Platzhalter für das zu erstellende Listenobjekt steht, z. B. Schnittstelle). Dies öffnet ein Dialogfeld, in welchem Sie die Eigenschaften des Objektes festlegen können.

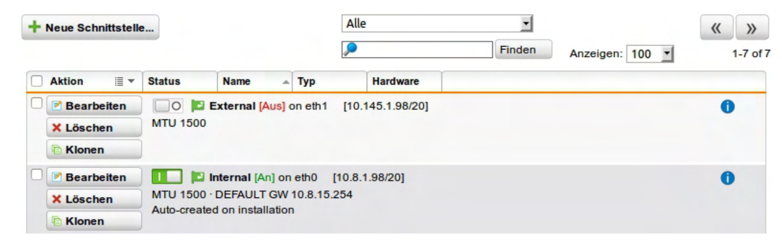


Bild 5 WebAdmin: Beispiel einer Liste

Mit der ersten Auswahlliste über der Liste können Sie die Listeneinträge nach ihrem Typ oder ihrer Gruppe sortieren. Die zweite Auswahlliste dient der gezielten Suche nach Listeneinträgen. Geben Sie dazu einen Suchbegriff ein und klicken Sie auf *Finden*.

Listen mit mehr als zehn Einträgen sind auf mehrere Seiten aufgeteilt. Mit den Schaltflächen Vorwärts (>>) und Rückwärts (<<) können Sie zwischen den Seiten hin- und herschalten. Mit der Auswahlliste *Anzeige* können Sie die Anzahl der Einträge pro Seite vorübergehend ändern. Zudem können Sie die Standardeinstellung für alle Listen auf der Registerkarte *Verwaltung > WebAdmin-Einstellungen > Benutzereinstellungen* ändern.

Mit Listenüberschriften können einige Funktionen ausgeführt werden. Wenn Sie eine Listenüberschrift anklicken, wird die Liste normalerweise nach dem entsprechenden Objektfeld sortiert. Wenn Sie beispielsweise auf das Feld *Name* klicken, wird die Liste nach den Namen der Objekte sortiert. Das Feld *Aktion* in der Überschrift bietet mehrere Batch-Optionen, die Sie für zuvor ausgewählte Listenobjekte durchführen können. Um Objekte auszuwählen, markieren Sie die zugehörigen Auswahlkästchen. Beachten Sie, dass die Auswahl seitenübergreifend gültig bleibt, d. h., wenn Sie durch die Seiten einer Liste blättern, bleiben bereits ausgewählte Objekte ausgewählt.

Tipp – Durch einen Klick auf das Infosymbol eines Listeneintrags können Sie sehen, in welchen Konfigurationen das Objekt verwendet wird.

2.4 Suche in Listen

Über das Filterfeld lässt sich die Anzahl der in einer Liste angezeigten Einträge schnell reduzieren. Dadurch wird es wesentlich einfacher, die Objekte zu finden, die Sie suchen.

Wissenswertes

- Während einer Suche werden normalerweise mehrere Felder nach dem Suchausdruck durchsucht. Eine Suche in `Benutzer & Gruppen` berücksichtigt beispielsweise Benutzername, Realname, Kommentar und erste E-Mail-Adresse. Allgemein gesagt berücksichtigt die Suche alle Texte, die Sie in der Liste sehen können, ausgenommen jene Details, die nach einem Klick auf das Infosymbol angezeigt werden.

- Die Listensuche ignoriert Groß-/Kleinschreibung. Das bedeutet, dass es keinen Unterschied macht, ob Sie Groß- oder Kleinbuchstaben eingeben. Das Suchergebnis wird Übereinstimmungen sowohl mit Groß- als auch mit Kleinbuchstaben anzeigen. Sie

können nicht explizit nach Groß- oder Kleinbuchstaben suchen.

- Die Listensuche basiert auf Perl-kompatiblen regulären Ausdrücken (abgesehen von der Groß-/Kleinschreibung). Typische, aus Texteditoren bekannte Suchausdrücke wie * und ? (als einfache Platzhalter) sowie die Operanden AND und OR funktionieren *nicht* in der Listensuche.

Beispiele

Die folgende Liste stellt eine kleine Auswahl nützlicher Suchausdrücke dar:

Einfacher Ausdruck: Liefert alle Wörter zurück, die den angegebenen Ausdruck enthalten. Beispielsweise findet „inter“ die Ergebnisse „Internet“, „interface“ und „printer“.

Wortanfang: Stellen Sie dem Suchausdruck die Zeichenfolge `\b` voran.Beispielsweise findet `\binter` die Ergebnisse „Internet“ und „Interface“, nicht jedoch „Printer“.

Wortende: Hängen Sie hinten an den Suchausdruck die Zeichenfolge `\b` an.Beispielsweise findet `http\b` das Ergebnis „http“, nicht jedoch „https“.

Beginn eines Eintrags: Stellen Sie dem Suchausdruck das Zeichen `^` voran.Beispielsweise findet `^inter` das Ergebnis „Internet Uplink“, nicht jedoch „Uplink Interfaces“.

IP-Adressen: Wenn Sie nach IP-Adressen suchen, müssen Sie die Trennpunkte mit einem Backslash (umgekehrter Schrägstrich) maskieren. Um nach `192\.168` zu suchen, müssen Sie beispielsweise „192.168“ eingeben.
Für eine allgemeinere Suche nach IP-Adressen verwenden Sie `\d` als Platzhalter für eine beliebige Ziffer. `\d+` findet mehrere aufeinander folgende Ziffern.Mit `\d+\.\d+\.\d+\.\d+` findet man beispielsweise jede beliebige IPv4-Adresse.

Hinweis – Es ist sinnvoller, einen einfacheren, sicheren Suchausdruck zu verwenden, der zu mehr Ergebnissen führt, als sich den Kopf über den perfekten Suchausdruck zu zerbrechen, welcher dann eher zu unerwarteten Ergebnissen oder falschen Schlussfolgerungen führt.

Eine ausführliche Beschreibung regulärer Ausrücke und deren Verwendung in Sophos UTM finden Sie in der Sophos-Knowledgebase.

2.5 Dialogfelder

Dialogfelder sind spezielle Eingabemasken im WebAdmin, bei denen Sie aufgefordert sind, bestimmte Informationen einzugeben. Das Beispiel zeigt ein Dialogfeld für das Anlegen einer statischen Route im Menü *Schnittstellen & Routing* > *Statisches Routing*.



Bild 6 WebAdmin: Beispiel eines Dialogfelds

Jedes Dialogfeld kann aus verschiedenen Kontrollelementen (Widgets) wie zum Beispiel Textfeldern oder Auswahlkästchen bestehen. Viele Dialogfelder bieten darüber hinaus eine Drag-and-Drop-Funktionalität, was durch einen speziellen Hintergrund mit dem Schriftzug *DND* gekennzeichnet ist. Immer dann, wenn Sie ein solches Feld vorfinden, können Sie ein Objekt durch Ziehen und Ablegen mit der Maus (Drag-and-Drop) in dieses Feld ziehen. Um die Objektliste zu öffnen, von der aus Sie das Objekt in das Feld ziehen können, klicken Sie auf das gelbe Ordnersymbol direkt neben dem Textfeld. Abhängig von der jeweiligen Konfigurationsoption öffnet sich die Liste mit den verfügbaren Netzwerk-, Dienst-, Benutzer-/Gruppen- oder Zeitraumdefinitionen. Ein Klick auf das grüne Plussymbol öffnet ein Dialogfenster, in welchem Sie eine neue Definition anlegen können. Einige Kontrollelemente, die für eine bestimmte Konfiguration nicht benötigt werden, sind ausgegraut. In manchen Fällen können diese durchaus editiert werden, haben dann allerdings keinen Effekt.

Hinweis – Im WebAdmin gibt es u. a. die Schaltflächen *Speichern* und *Übernehmen*. Die Schaltfläche *Speichern* wird immer dann angezeigt, wenn Sie ein Objekt in WebAdmin neu anlegen oder bearbeiten, zum Beispiel, wenn Sie eine neue statische Route anlegen oder Netzwerkdefinitionen bearbeiten. Sie wird immer zusammen mit einer Schaltfläche *Abbrechen* angezeigt. Die Schaltfläche *Übernehmen* hingegen dient dazu, Ihre Einstellungen in das Backend zu übertragen und dadurch sofort wirksam werden zu lassen.

2.6 Schaltflächen und Symbole

Der WebAdmin verfügt über einige Schaltflächen und Symbole mit hinterlegter Funktion, deren Nutzung hier beschrieben wird.

Schaltflächen	Bedeutung
Anschauen	Zeigt ein Dialogfeld mit detaillierten Informationen zum Objekt an.
Bearbeiten	Öffnet ein Dialogfeld, in dem die Eigenschaften des Objekts bearbeitet werden können.
Löschen	Löscht das Objekt. Es wird eine Warnung ausgegeben, wenn ein Objekt noch irgendwo anders benutzt wird. Nicht alle Objekte können gelöscht werden, wenn sie in Benutzung sind.
Klonen	Öffnet ein Dialogfeld, um ein Objekt mit identischen Einstellungen/Eigenschaften anzulegen. Klonen dient dazu, ähnliche Objekte anzulegen, ohne alle identischen Einstellungen erneut eingeben zu müssen.

Symbole mit Funktion	Bedeutung
	Info: Zeigt alle Konfigurationen an, in denen das Objekt verwendet wird.
	Details: Verlinkt auf eine andere WebAdmin-Seite mit weiteren Informationen zu diesem Thema.
	Schieberegler: Aktiviert oder deaktiviert eine Funktion. Er zeigt Grün an, wenn die Funktion aktiv ist, Grau, wenn die Funktion deaktiviert ist, und Gelb, wenn eine Konfigurierung nötig ist, bevor die Funktion aktiviert werden kann.
	Ordner: Hat zwei Funktionen: (1) Öffnet eine Objektleiste (siehe Abschnitt unten) auf der linken Seite, aus der Sie passende Objekte auswählen können. (2) Öffnet ein Dialogfenster, um eine Datei hochzuladen.
	Plus: Öffnet ein Dialogfenster, um ein neues Objekt des erforderlichen Typs hinzuzufügen.

Symbole mit Funktion	Bedeutung
	Aktion: Öffnet eine Auswahlliste mit Aktionen. Die Aktionen hängen davon ab, wo sich das Symbol befindet: (1) Symbol in Listenüberschrift: Die Aktionen, z. B. *Aktivieren*, *Deaktivieren* oder *Löschen*, gelten für die ausgewählten Listenobjekte.(2) Symbol in Textfeld: Mit den Aktionen *Import* und *Export* können Sie Text importieren oder exportieren und mit *Leeren* den gesamten Inhalt löschen. Außerdem existiert ein Filterfeld, mit dem Sie eine Liste auf die relevanten Elemente reduzieren können. Beachten Sie, dass der Filter zwischen Groß- und Kleinschreibung unterscheidet.
	Leeren: Entfernt ein Objekt aus der aktuellen Konfiguration, wenn es sich vor dem Objekt befindet. Entfernt alle Objekte aus einem Feld, wenn es sich im Menü *Aktionen* befindet. Objekte werden jedoch niemals gelöscht.
	Import: Öffnet ein Dialogfenster, um Text mit mehr als einem Eintrag bzw. mehr als einer Zeile zu importieren. Diese Funktion erleichtert das Hinzufügen von mehreren Einträgen auf einmal, ohne diese einzeln eingeben zu müssen, z. B. einer langen Negativliste (Blacklist) zur URL-Negativliste. Kopieren Sie den Text dazu aus einer beliebigen Ausgangsdatei und fügen Sie ihn mittels `Strg+V` ein.
	Export: Öffnet ein Dialogfenster, um alle vorhandenen Einträge zu exportieren. Sie können als Trennzeichen entweder Zeilenumbruch, Doppelpunkt oder Komma wählen, um Einträge voneinander zu trennen. Um Einträge als Text zu exportieren, markieren Sie den ganzen Text im Feld *Exportierter Text* und drücken Sie `Strg+C`, um ihn zu kopieren.Sie können ihn dann mittels `Strg+V` in allen üblichen Anwendungen, z. B. einem Texteditor, einfügen.
	Sortieren: Mithilfe dieser beiden Pfeile können Sie Listenelemente sortieren, indem Sie ein Element in der Liste nach oben oder unten verschieben.
« »	**Vorwärts/Rückwärts:** Mithilfe dieser beiden Pfeile können Sie je nach Ihrer Position durch die Seiten einer langen Liste navigieren oder entlang eines Änderungs- und Einstellungsverlaufs vor- und zurücknavigieren.
PDF	**PDF:** Speichert die aktuelle Ansicht der Daten in einer PDF-Datei und öffnet anschließend ein Dialogfenster, um die erzeugte Datei herunterzuladen.
XLS	**CSV:** Speichert die aktuelle Ansicht der Daten in einer CSV-Datei (durch Komma getrennte Werte) und öffnet anschließend ein Dialogfenster, um die erzeugte Datei herunterzuladen.

2.7 Objektlisten

Eine Objektliste ist eine Liste von Objekten die gelegentlich auf der linken Seite des WebAdmin eingeblendet wird und dabei vorübergehend das Hauptmenü verdeckt.

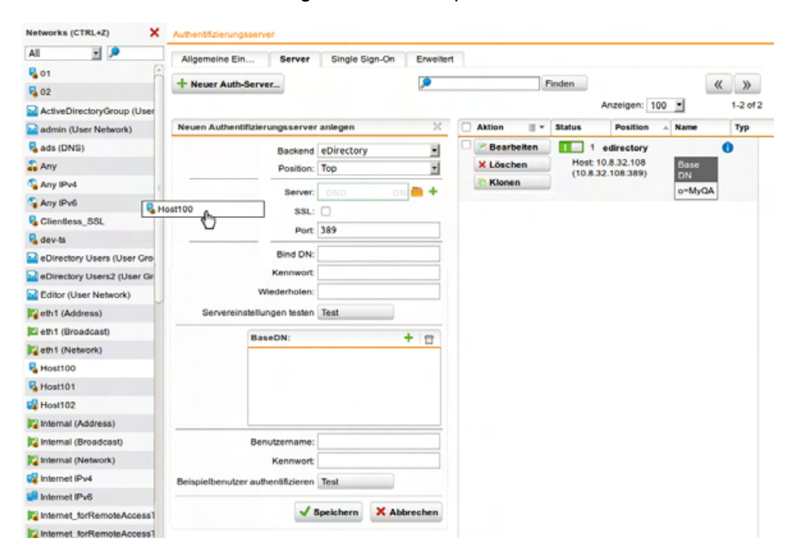


Bild 7 WebAdmin: Ziehen eines Objekts aus der Objektliste *Networks*

Eine Objektliste wird automatisch geöffnet, wenn Sie auf das Ordnersymbol klicken (siehe Abschnitt oben). Sie kann auch manuell über ein Tastaturkürzel geöffnet werden (siehe *Verwaltung > WebAdmin-Einstellungen > Benutzereinstellungen*).
Die Objektliste ermöglicht einen schnellen Zugriff auf WebAdmin-Objekte wie Benutzer/Gruppen, Schnittstellen, Netzwerke und Dienste, um sie für Konfigurationszwecke auswählen zu können. Objekte werden ausgewählt, indem sie einfach zur aktuellen Konfiguration gezogen und dort über dem entsprechenden Feld fallen gelassen werden (Drag and Drop).
Es gibt fünf verschiedene Arten von Objektlisten, entsprechend den Objekttypen, die es gibt. Bei einem Klick auf das Ordnersymbol wird immer die Objektliste geöffnet, deren Typ von der aktuellen Konfiguration benötigt wird.

3 Dashboard

Das Dashboard zeigt eine grafische Momentaufnahme des Betriebsstatus von Sophos UTM.

Das Dashboard wird standardmäßig nach der Anmeldung am WebAdmin angezeigt und stellt die folgenden Informationen zur Verfügung:

Tipp – Wenn Sie auf das Symbol „Dashboard-Einstellungen" oben rechts klicken, wird ein Dialogfenster geöffnet, in dem Sie unter anderem auswählen können, welche Themenabschnitte angezeigt werden sollen.

- **Allgemeine Informationen:** Hostname, Modell, Lizenz-ID, Abonnements und die Zeitspanne, für die das Gerät in Betrieb ist. Die Farbe, in der ein Abonnement angezeigt wird, wechselt 30 Tage vor Ablaufdatum auf orange. In den letzten 7 Tagen vor Ablauf sowie nach Ablauf wird das Abonnement rot angezeigt.
- **Versionsinformationen:** Informationen zu den aktuell installierten Firmware- und Patternversionen sowie verfügbaren Updates.
- **Ressourcennutzung:** Aktuelle Systemauslastung, insbesondere der folgenden Komponenten:
  - Die CPU-Auslastung in Prozent
  - Die RAM-Auslastung in Prozent Hinweis: Der angezeigte Gesamtspeicher ist der Teil, der für das Betriebssystem nutzbar ist. Bei 32-Bit-Systemen entspricht dies manchmal nicht der tatsächlichen Größe des installierten physischen Speichers, da ein Teil davon für Hardware reserviert ist.
  - Der von der Protokollpartition belegte Festplattenplatz in Prozent
  - Der von der Root-Partition belegte Festplattenplatz in Prozent
  - Der Status des USV-Gerätes (unterbrechungsfreie Stromversorgung) (falls vorhanden)
- **Heutiger Bedrohungsstatus:** Ein Zähler für die wichtigsten registrierten Bedrohungen seit Mitternacht:
  - Die Summe der Datenpakete, die vom Paketfilter verworfen (engl. drop) oder abgelehnt (engl. reject) wurden und für die Protokollierung aktiviert ist
  - Die Summe der blockierten Angriffsversuche
  - Die Summe der blockierten Viren (alle Proxies)

  - Die Summe der blockierten Spam-Nachrichten (SMTP/POP3)
  - Die Summe der blockierten Spyware (alle Proxies)
  - Die Summe der blockierten URLs (HTTP/S)
  - Die Summe der blockierten Webserver-Angriffe (WAF)

- **Schnittstellen:** Name und Status von konfigurierten Netzwerkkarten.Darüber hinaus wird für jede Schnittstelle die durchschnittliche Datenübertragungsrate der letzten 75 Sekunden für ein- und ausgehenden Datenverkehr angezeigt. Die Werte resultieren aus Durchschnittswerten, die in Intervallen von 15 Sekunden gewonnen werden. Ein Klick auf einen Verkehrswert einer Schnittstelle öffnet den Flow-Monitor in einem neuen Fenster. Der Flow-Monitor zeigt den Datenverkehr der letzten zehn Minuten an und aktualisiert sich selbst in kurzen Abständen.Weitere Informationen zum Flow-Monitor finden Sie im Kapitel *Flow-Monitor*.
- **Advanced Threat Protection:** Status von Advanced Threat Protection. Die Ansicht zeigt, ob Advanced Threat Protection aktiviert ist, und einen Zähler infizierter Hosts.
- **Aktuelle Systemkonfiguration:** Anzeige der wichtigsten Sicherheitsfunktionen und deren Aktivitätsstatus.Wenn Sie auf einen der Einträge klicken, öffnet sich die WebAdmin-Seite mit den entsprechenden Einstellungen:
  - **Firewall:** Informationen zu allen aktiven Firewallregeln.
  - **Angriffschutz:** Das Angriffschutzsystem (IPS, Intrusion Prevention System) erkennt Angriffsversuche anhand eines signaturbasierten IPS-Regelwerks.
  - **Webfilter:** Ein Gateway auf Anwendungsebene für das HTTP/S-Protokoll, das eine große Auswahl an Filtermechanismen für die Netzwerke bietet, die seine Dienste verwenden dürfen.
  - **Netzwerksichtbarkeit:**Sophos-Layer-7-Application-Control ermöglicht die Kategorisierung und Kontrolle von Netzwerkverkehr.
  - **SMTP-Proxy:** Ein Gateway auf Anwendungsebene für Nachrichten, die über das *Simple Mail Transfer Protocol* (SMTP) gesendet werden.
  - **POP3-Proxy:** Ein Gateway auf Anwendungsebene für Nachrichten, die über das *Post Office Protocol 3* (POP3) gesendet werden.
  - **RED:** Konfiguration von Remote-Ethernet-Device-(RED)-Appliances für die Sicherheit von Zweigniederlassungen.
  - **Wireless Protection:** Konfiguration von kabellosen Netzwerken und Access Points.

- **Endpoint Protection:** Verwaltung von Endpoint-Geräten in Ihrem Netzwerk. Zeigt die Anzahl der verbundenen Endpoints und Warnungen an.
- **Site-to-Site-VPN:** Konfiguration von Site-to-Site-VPN-Verbindungen.
- **Fernzugriff:** Konfiguration von VPN-Szenarien für Road Warriors.
- **Web Application Firewall:** Ein Gateway auf Anwendungsebene zum Schutz Ihrer Webserver vor Angriffen wie Cross-Site-Scripting und SQL-Injections.
- **HA/Cluster:** Ausfallsicherheit und Cluster-Technologie, d. h. die gleichmäßige Verteilung von rechenintensiven Aufgaben wie z. B. dem Filtern von Inhalten, Virenscans, Angriffschutz oder Entschlüsselung auf mehrere Computer.
- **Sophos UTM Manager:** Verwaltung Ihrer Sophos UTM-Appliance über das zentrale Verwaltungs-Tool Sophos UTM Manager (SUM).
- **Antivirus:** Schutz Ihres Netzwerks vor Internetverkehr, der schädlichen Inhalt wie Viren, Würmer und andere Schadsoftware verbreitet.
- **Antispam:** Erkennung von unerwünschten E-Mails und Spam-Übermittlung von bekannten oder verdächtigen Spam-Versendern.
- **Antispyware:** Schutz vor Spyware-Infektionen durch zwei unabhängig voneinander operierende Virenscanner, deren Virensignaturen- und Spyware-Filtermechanismen regelmäßig aktualisiert werden und eingehenden sowie ausgehenden Datenverkehr schützen.

3.1 Dashboard-Einstellungen

Sie können diverse Dashboard-Einstellungen vornehmen. Klicken Sie oben rechts im Dashboard auf das Symbol Dashboard-Einstellungen, um das Dialogfenster *Dashboard-Einstellungen bearbeiten* zu öffnen.

Dashboard aktualisieren: Standardmäßig wird das Dashboard alle fünf Sekunden aktualisiert. Das Zeitintervall für die Aktualisierung kann von *Nie* bis zu *Jede Minute* eingestellt werden.

Linke Spalte – Rechte Spalte: Das Dashboard ist in verschiedene Themenbereiche untergliedert, in denen Sie Informationen zum jeweiligen Thema finden.Mit den beiden Feldern *Linke Spalte* und *Rechte Spalte* können Sie die Themenabschnitte neu anordnen, Themenabschnitte hinzufügen oder aus dem Anzeigebereich entfernen. Diese Einstellungen werden auf das Dashboard angewendet. Verwenden Sie die Sortier-Symbole um die

Themenabschnitte einer Spalte zu sortieren. Um einen bestimmten Themenabschnitt zum Anzeigebereich hinzuzufügen oder daraus zu entfernen, aktivieren bzw. deaktivieren Sie das zugehörige Auswahlkästchen.

Die standardmäßig angezeigten Themenabschnitte werden im Kapitel „Dashboard“ beschrieben. Es gibt einige weitere Themenabschnitte, die angezeigt werden können. Sie sind im Folgenden beschrieben:

- **Web Protection: Häufigste Anwendungen:** Überblick über die am häufigsten verwendeten Anwendungen. Wenn Sie in diesem Themenabschnitt mit dem Mauszeiger über eine Anwendung fahren, werden ein oder zwei Symbole mit zusätzlichen Funktionen angezeigt:
  - Klicken Sie auf das Symbol *Blockieren*, um die Anwendung ab diesem Moment zu blockieren. Auf der Seite *Application-Control-Regeln* wird dann eine Regel erstellt. Diese Option ist nicht für Anwendungen verfügbar, die für einen reibungslosen Betrieb von Sophos UTM relevant sind. So kann beispielsweise WebAdmin-Datenverkehr nicht blockiert werden, da dies dazu führen könnte, dass Sie nicht mehr auf den WebAdmin zugreifen können. Auch nicht klassifizierter Datenverkehr kann nicht blockiert werden.
  - Klicken Sie auf das Symbol *Regeln*, um Traffic Shaping für die entsprechende Anwendung zu aktivieren.Ein Dialogfenster wird geöffnet, in dem Sie die Regeleinstellungen vornehmen können. Klicken Sie auf *Speichern*, wenn Sie fertig sind. Dies erstellt jeweils eine Regel auf den Seiten *Verkehrskennzeichner* und *Bandbreiten-Pools*.
    Traffic-Shaping ist nicht verfügbar, wenn Sie eine Flow-Monitor-Ansicht mit *allen Schnittstellen* ausgewählt haben, da Traffic-Shaping schnittstellenbasiert funktioniert.
- **Web Protection: Häufigste Sites nach Tageszeit:** Überblick über die am häufigsten besuchten Domänen im Zeitverlauf.
- **Web Protection: Häufigste Seiten nach Datenverkehr:** Überblick über die am häufigsten besuchten Domänen nach Datenverkehr.
- **Protokollierung:** Status der Protokollpartition von Sophos UTM, einschließlich Informationen zum freien Festplattenspeicherplatz und zur Zuwachsrate.
- **Newsfeed:** Neuigkeiten zu Sophos und seinen Produkten.
- **Diagramm: Gleichzeitige Verbindungen:** Tägliche Statistiken und Histogramm der Gesamtzahl an gleichzeitigen Verbindungen.

- **Diagramm: Protokollpartitionsstatus:** Statistik und Histogramm der Protokollpartitionsauslastung für vier Wochen.
- **Diagramm: CPU-Auslastung:** Tägliche Statistiken und Histogramm der aktuellen Prozessorauslastung in Prozent.
- **Diagramm: Speicher-/Swap-Auslastung:** Tägliche Statistiken und Histogramm der Speicher- und Swap-Auslastung in Prozent.
- **Diagramm: Auslastung der Speicherpartition:** Tägliche Statistiken und Histogramm der Auslastung ausgewählter Speicherpartitionen in Prozent.

Autogruppierung in Dashboard aktivieren: Wählen Sie diese Option, um Informationen im Dashboard kompakt anzuzeigen. Diese Option betrifft nur die ausgewählten *Web-Protection*-Elemente in der linken Spalte und die ausgewählten *Diagramm*-Elemente in der rechten Spalte. Wenn diese Option ausgewählt ist, werden die jeweiligen Informationselemente als überlappende Registerkarten im Dashboard angezeigt. Ist sie nicht ausgewählt, werden die Informationselemente nebeneinander angezeigt.

Klicken Sie auf *Speichern*, um Ihre Einstellungen zu speichern.

3.2 Flow-Monitor

Der Flow-Monitor von Sophos UTM ist eine Anwendung, die schnellen Zugriff auf Informationen zum aktuellen Datenverkehr bietet, der die Schnittstellen von UTM passiert. Der Zugriff erfolgt ganz einfach über das Dashboard durch einen Klick auf eine der Schnittstellen oben rechts. Wenn Sie auf *Alle Schnittstellen* klicken, zeigt der Flow-Monitor den gesamten Datenverkehr auf allen aktiven Schnittstellen an. Wenn Sie auf eine einzelne Schnittstelle klicken, zeigt der Flow-Monitor nur den Datenverkehr dieser Schnittstelle an.

Hinweis – Der Flow-Monitor wird in einem neuen Browser-Fenster geöffnet. Da das Fenster möglicherweise von Popup-Blockern blockiert wird, ist es ratsam, Popup-Blocker für den WebAdmin zu deaktivieren.

Der Flow-Monitor bietet mit einem Diagramm und einer Tabelle zwei Ansichten, die in den nächsten Abschnitten beschrieben werden. Die Anwendung wird alle fünf Sekunden aktualisiert.Sie können auf die Schaltfläche *Pause* klicken, um die Aktualisierung zu unterbrechen. Wenn Sie auf *Weiter* klicken, um die Aktualisierung wieder aufzunehmen, aktualisiert der Flow-Monitor die Daten, sodass der aktuelle Datenverkehr angezeigt wird.

Diagrammansicht

Das Flow-Monitor-Diagramm zeigt den Netzwerkverkehr der letzten zehn Minuten an. Die horizontale Achse zeigt die Zeit und die vertikale Achse den Umfang des Datenverkehrs, wobei die Skala dynamisch an den Durchsatz angepasst wird.

In der Diagrammansicht unten wird eine Legende angezeigt, die Informationen zur Art des Datenverkehrs auf einer Schnittstelle bietet. Jeder Art von Datenverkehr ist eine andere Farbe zugewiesen, sodass eine Unterscheidung des im Diagramm angezeigten Datenverkehrs problemlos möglich ist.

Hinweis – Der Flow-Monitor zeigt wesentlich genauere Informationen zum Datenverkehr an, wenn Netzwerksichtbarkeit aktiviert ist (siehe Kapitel *Web Protection > Application Control > Netzwerksichtbarkeit*).

Wenn Sie mit dem Mauszeiger über das Diagramm fahren, wird ein Punkt angezeigt, der Ihnen detaillierte Informationen zu diesem Teil des Diagramms liefert. Der Punkt haftet an der Linie des Diagramms. Er folgt den Bewegungen des Mauszeigers. Wenn ein Diagramm mehrere Linien hat, wechselt der Punkt zwischen ihnen, je nachdem, wohin Sie den Mauszeiger bewegen. Darüber hinaus ändert der Punkt seine Farbe in Abhängigkeit davon, auf welche Linie sich seine Informationen beziehen. Das ist besonders nützlich, wenn Linien eng nebeneinander liegen.Der Punkt bietet Informationen zu Art und Größe des Datenverkehrs zum jeweiligen Zeitpunkt.

Tabellarische Ansicht

Die Flow-Monitor-Tabelle bietet Informationen zum Netzwerkverkehr der letzten fünf Sekunden:

#: Der Datenverkehr wird nach der aktuellen Bandbreitennutzung angeordnet.

Anwendung: Protokoll oder Name des Netzwerkverkehrs, falls verfügbar. Nicht klassifizierter Datenverkehr ist eine dem System unbekannte Art des Datenverkehrs. Nach einem Klick auf eine Anwendung wird ein Fenster geöffnet, das Informationen über den Server, den verwendeten Port, die benötigte Bandbreite pro Serververbindung und den gesamten Datenverkehr anzeigt.

Clients: Anzahl der Clientverbindungen, die die Anwendung nutzen. Nach einem Klick auf einen Client wird ein Fenster geöffnet, das Informationen über die IP-Adresse des Clients, die benötigte Bandbreite pro Clientverbindung und den Gesamtverkehr anzeigt. Beachten Sie, dass bei nicht klassifiziertem (unclassified) Verkehr die Anzahl der Clients in der Tabelle höher sein kann als im zusätzlichen Informationsfenster. Das liegt daran, dass die Bezeichnung „unclassified" mehr als eine Anwendung einschließt. Daher ist es möglich, dass im Informationsfenster nur ein Client, in der Tabelle jedoch drei Clients aufgeführt werden. Bei letzteren handelt es sich eigentlich um die Verbindungen des einen Clients mit drei verschiedenen, nicht klassifizierten Anwendungen.

Aktuelle Bandbreitennutzung: Die Bandbreitennutzung der letzten fünf Sekunden. Nach einem Klick auf eine Bandbreite wird ein Fenster geöffnet, das Informationen zur Download- und Upload-Rate der Anwendungsverbindung anzeigt.

Gesamter Datenverkehr: Der gesamte Datenverkehr einer Verbindung, solange diese besteht. Beispiel 1: Ein Download wurde vor einiger Zeit gestartet und ist noch nicht beendet: Der gesamte Datenverkehr seit dem Beginn des Downloads wird angezeigt. Beispiel 2: Mehrere Clients nutzen Facebook: Solange ein Client die Verbindung offen hält, wird der gesamte bisher von allen Clients verursachte Datenverkehr angezeigt.
Nach einem Klick auf den gesamten Datenverkehr wird ein Fenster geöffnet, das Informationen zur Download- und Upload-Rate der Anwendungsverbindung anzeigt.

Aktionen: Je nach Typ der Anwendung können verschiedene Aktionen durchgeführt werden (außer bei nicht klassifiziertem Verkehr).

- Blockierung: Klicken Sie auf die Schaltfläche *Blockieren*, um die Anwendung ab diesem Moment zu blockieren. Auf der Seite *Application-Control-Regeln* wird dann eine Regel erstellt. Diese Option ist nicht für Anwendungen verfügbar, die für einen reibungslosen Betrieb von Sophos UTM relevant sind. So kann beispielsweise WebAdmin-Datenverkehr nicht blockiert werden, da dies dazu führen könnte, dass Sie nicht mehr auf den WebAdmin zugreifen können. Auch nicht klassifizierter Datenverkehr kann nicht blockiert werden.
- Traffic-Shaping: Klicken Sie auf die Schaltfläche *Regeln*, um Traffic Shaping für die entsprechende Anwendung zu aktivieren. Ein Dialogfenster wird geöffnet, in dem Sie die Regeleinstellungen vornehmen können. Klicken Sie auf *Speichern*, wenn Sie fertig sind. Dies erstellt jeweils eine Regel auf den Seiten *Verkehrskennzeichner* und *Bandbreiten-Pools*.
  Traffic-Shaping ist nicht verfügbar, wenn Sie eine Flow-Monitor-Ansicht mit *allen Schnittstellen* ausgewählt haben, da Traffic-Shaping schnittstellenbasiert funktioniert.

- Download-Drosselung: Klicken Sie auf die Schaltfläche *Throttle*, um Download-Drosselung für die entsprechende Anwendung zu aktivieren. Ein Dialogfenster wird geöffnet, in dem Sie die Regeleinstellungen vornehmen können. Klicken Sie auf *Speichern*, wenn Sie fertig sind.Hiermit wird jeweils eine Regel auf den Seiten *Verkehrskennzeichner* und *Download-Drosselung* hinzugefügt. Download-Drosselung ist nicht verfügbar, wenn Sie eine Flow-Monitor-Ansicht mit *allen Schnittstellen* ausgewählt haben, da Download-Drosselung schnittstellenbasiert funktioniert.

4 Verwaltung

In diesem Kapitel wird beschrieben, wie grundlegende Systemeinstellungen sowie Einstellungen für die Web-basierte, administrative Benutzeroberfläche von Sophos UTM, *WebAdmin*, vorgenommen werden. Die Seite *Verwaltungsübersicht* zeigt eine Statistik der letzten Anmeldungen am WebAdmin inklusive der gegebenenfalls durchgeführten Änderungen. Klicken Sie auf die Schaltfläche *Anzeigen* in der Spalte *Änderungsprotokoll*, um die Änderungen im Detail zu sehen.

In der Spalte *Status* ist aufgelistet, wann frühere WebAdmin-Sitzungen beendet wurden.

Hinweis – Sie können WebAdmin-Sitzungen beenden, indem Sie auf das Menü *Abmelden* klicken. Wenn Sie den Browser schließen, ohne auf das Menü *Abmelden* zu klicken, läuft die Sitzung nach der Zeitspanne aus, die auf der Registerkarte *Verwaltung* > *WebAdmin-Einstellungen* > *Erweitert* festgelegt ist.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Systemeinstellungen
- WebAdmin-Einstellungen
- Lizenzen
- Up2Date
- Backup/Wiederherstellen
- Benutzerportal
- Benachrichtigungen
- Anpassungen
- SNMP
- Zentrale Verwaltung
- High Availabilty (Hochverfügbarkeit)
- Ausschalten/Neustart

4.1 Systemeinstellungen

Über die Registerkarten im Menü *Systemeinstellungen* können grundlegende Einstellungen Ihrer UTM, u. a. Hostname, Datum und Uhrzeit, vorgenommen werden.

4.1.1 Organisatorisches

Geben Sie den Namen, den Ort Ihrer Organisation und eine E-Mail-Adresse ein, über die eine Person oder Gruppe erreicht werden kann, die die technische Verantwortung für Ihre Sophos UTM trägt. Diese Informationen werden auch in Zertifikaten für IPsec, Email Encryption und den WebAdmin verwendet.

4.1.2 Hostname

Geben Sie den Hostnamen Ihrer UTM als *Fully Qualified Domain Name* (FQDN) in dieses Feld ein, z. B. `utm.beispiel.de`. Ein Hostname darf aus alphanumerischen Zeichen, Punkten und Bindestrichen bestehen. Am Ende des Hostnamens muss ein spezieller Bezeichner wie z. B. `com`, `org` oder `de` stehen. Der Hostname wird u. a. in Benachrichtigungs-E-Mails verwendet, um die UTM zu identifizieren. Der Hostname erscheint auch in Statusmeldungen des Webfilters. Beachten Sie, dass der Hostname nicht in der DNS-Zone für Ihre Domäne registriert werden muss.

4.1.3 Zeit und Datum

Auf Ihrer UTM sollten Datum und Uhrzeit immer richtig eingestellt sein. Dies ist eine Voraussetzung dafür, dass die Informationen in den Protokoll- und Berichtssystemen korrekt sind und dass die Zusammenarbeit mit anderen Computern im Internet problemlos abläuft.

Üblicherweise brauchen Sie Zeit und Datum nicht manuell einzustellen. Denn standardmäßig ist die automatische Synchronisierung mit öffentlichen Internetzeitservern aktiviert (siehe Abschnitt *Synchronisierung der Systemzeit mit NTP* unten).

In dem unwahrscheinlichen Fall, dass Sie die Synchronisierung mit Zeitservern deaktivieren müssen, können Sie Zeit und Datum manuell ändern. Wenn Sie das tun, beachten Sie aber die folgenden wichtigen Hinweise:

- Ändern Sie niemals die Zeit von Winterzeit auf Sommerzeit oder andersherum. Diese Änderung wird immer automatisch durch die eingestellte Zeitzone durchgeführt, auch wenn die automatische Synchronisierung mit Zeitservern deaktiviert ist.
- Ändern Sie nie Datum oder Zeit, während die Synchronisierung mit Zeitservern noch aktiviert ist, da die automatische Synchronisierung Ihre Änderungen immer sofort wieder rückgängig machen wird. Falls Sie Datum oder Zeit manuell einstellen müssen, denken Sie daran, zuerst alle Server aus dem Feld *NTP-Server* im Abschnitt *Synchronisierung der Systemzeit mit NTP* zu entfernen und dann auf *Übernehmen* zu klicken.
- Nachdem Sie die Zeit manuell geändert haben, warten Sie, bis Sie eine grüne Bestätigungsmeldung sehen, die besagt, dass die Änderung erfolgreich war.Starten Sie danach das System neu (*Verwaltung > Ausschalten/Neustart*). Das ist sehr empfehlenswert, da viele Dienste darauf vertrauen, dass sich die Zeit fortlaufend und nicht plötzlich ändert. Zeitsprünge können daher zu Fehlfunktionen bei einigen Diensten führen. Dieser Hinweis gilt für alle Arten von Computersystemen.
- In seltenen Fällen kann eine Änderung der Systemzeit sogar Ihre WebAdmin-Sitzung beenden. Falls das passiert, melden Sie sich erneut an, überprüfen Sie, ob die Zeit nun richtig eingestellt ist und starten Sie das System danach neu.

Falls Sie mehrere miteinander verbundene UTMs betreiben, die über verschiedene Zeitzonen reichen, wählen Sie eine gemeinsame Zeitzone, z. B. UTC (koordinierte Weltzeit). Damit lassen sich Protokolleinträge sehr viel einfacher vergleichen.

Wenn Sie die Systemzeit manuell ändern, beachten Sie, dass Ihnen einige Nebeneffekte begegnen werden, auch wenn Sie das System ordentlich neu gestartet haben.

- **Uhrzeit vorstellen**
  - In zeitbasierten Berichten fehlen Daten für die entsprechende Zeitspanne. Die meisten Diagramme stellen diesen Zeitraum als gerade Linie in Höhe des alten Wertes dar.
  - Für den Netzwerkverkehr (engl. Accounting) betragen alle Werte in dieser Zeitspanne 0.
- **Uhrzeit zurückstellen**
  - In den zeitbasierten Berichten gibt es für den entsprechenden Zeitraum bereits Protokolldaten (die aus Sicht des Systems aber aus der Zukunft stammen).
  - Die meisten Diagramme stellen die Werte dieser Zeitspanne komprimiert dar.
  - Die im Dashboard angezeigte verstrichene Zeit seit der letzten Pattern-Prüfung zeigt den Wert „nie“, obwohl die letzte Prüfung erst wenige Minuten zurückliegt.

- Automatisch auf der UTM erzeugte Zertifikate können ungültig werden, da der Beginn ihrer Gültigkeit aus Sicht des Systems in der Zukunft liegt.
- Berichtsdaten über den Netzwerkverkehr behalten die bereits erfassten Daten, obwohl sie in der Zukunft liegen. Sobald der Zeitpunkt der Zurücksetzung erreicht ist, werden die Netzwerkverkehr-Dateien weitergeschrieben.

Aufgrund dieser Nachteile sollten Sie die Systemzeit bei der Erstkonfiguration einmalig setzen und später nur geringfügig anpassen. Dies gilt insbesondere dann, wenn die gesammelten Netzwerkverkehrs- und Berichtsdaten weiterverarbeitet werden und die Genauigkeit der Daten wichtig ist.

Datum und Uhrzeit einstellen

Zur manuellen Konfiguration der Systemzeit wählen Sie Datum und Zeit aus den entsprechenden Auswahllisten aus. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Zeitzone einstellen

Um die Zeitzone des Systems zu ändern, wählen Sie ein Gebiet oder eine Zeitzone aus der Auswahlliste aus. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Das Ändern der Zeitzone ändert nicht die Systemzeit, sondern nur wie die Zeit ausgegeben wird, beispielsweise in Protokoll- und Berichtsdaten. Auch wenn dadurch keine Dienste unterbrochen werden, empfehlen wir dringend anschließend neu zu starten, um sicherzugehen dass alle Dienste die neue Zeiteinstellung verwenden.

Synchronisierung der Systemzeit mit NTP

Zur Synchronisierung der Systemzeit mithilfe eines Zeitservers wählen Sie einen oder mehrere NTP-Server aus. Klicken Sie auf *Übernehmen*, nachdem Sie die Konfiguration abgeschlossen haben.

NTP-Server: Der *NTP Server Pool* ist voreingestellt. Diese Netzwerkdefinition bezieht sich auf den großen virtuellen Zusammenschluss von öffentlichen Zeitservern des *pool.ntp.org*-Projekts. Falls Ihr Internetanbieter selbst NTP-Server für Kunden betreibt und Sie Zugang zu diesen Servern haben, ist es empfehlenswert, den *NTP Server Pool* zu entfernen und stattdessen die Server Ihres Anbieters zu verwenden. Wenn Sie Ihre eigenen oder die Server Ihres Anbieters verwenden, erhöht die Verwendung von mehr als einem Server die Präzision und Zuverlässigkeit. Die Verwendung von drei unabhängigen Servern ist eigentlich immer ausreichend. Die Verwendung von mehr als drei Servern bringt meistens keine weitere Verbesserung, erhöht hingegen die Serverlast. Es ist nicht empfehlenswert, sowohl den *NTP Server Pool* als

auch Ihre eigenen Server oder die Server Ihres Anbieters zu verwenden, da dies im Normalfall weder die Präzision noch die Zuverlässigkeit erhöht.

Tipp – Wenn Sie möchten, dass sich Client-Computer mit diesen NTP-Servern verbinden können, fügen Sie sie auf der Seite *Netzwerkdienste > NTP* zu den zugelassenen Netzwerken hinzu.

Konfigurierte Server testen: Klicken Sie auf diese Schaltfläche, um zu testen, ob mit den gewählten NTP-Servern eine Verbindung von Ihrem Gerät aus aufgebaut werden kann und ob verwendbare Zeitdaten vom Server empfangen werden. Dabei wird die Zeitverschiebung zwischen Ihrem System und den Servern ermittelt. Verschiebungen sollten normalerweise weit unter einer Sekunde liegen, wenn Ihr System korrekt konfiguriert ist und seit geraumer Zeit stabil funktioniert.

Direkt nachdem Sie NTP aktiviert oder andere Server hinzugefügt haben, ist es normal, wenn größere Verschiebungen auftreten. Um große Zeitsprünge zu vermeiden, verändert NTP die Systemzeit langsam Stück für Stück, sodass die Zeit ohne Sprünge korrigiert wird. Haben Sie in diesem Fall bitte Geduld. Starten Sie insbesondere in diesem Fall das System *nicht* neu. Schauen Sie lieber in einer Stunde noch einmal nach. Wenn sich die Verschiebung verringert, läuft alles so ab, wie es soll.

4.1.4 Shell-Zugriff

Secure Shell (SSH) ist ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf der UTM anmelden kann. Es wird typischerweise für Wartungsarbeiten und zur Fehlersuche verwendet. Für den Zugriff benötigen Sie einen SSH-Client, der in den meisten Linux-Distributionen enthalten ist.

Zugelassene Netzwerke

Verwenden Sie das Feld *Zugelassene Netzwerke*, um den SSH-Zugang auf bestimmte Netzwerke zu beschränken. Hier aufgeführte Netzwerke können sich am SSH-Dienst anmelden.

Authentifizierung

In diesem Abschnitt können Sie eine Authentifizierungsmethode für den SSH-Zugriff und die entsprechende Sicherheitsstufe festlegen. Die folgenden Authentifizierungsmethoden sind verfügbar:

- Kennwort (Standard)
- Öffentlicher Schlüssel
- Kennwort und öffentlicher Schlüssel

Um die Funktion *Authentifizierung mit öffentlichem Schlüssel zulassen* zu verwenden, müssen Sie für jeden Benutzer, der sich über seinen öffentlichen Schlüssel authentifizieren darf, den entsprechenden öffentlichen Schlüssel in das Feld *Autorisierte Schlüssel für loginuser* hochladen.

Root-Login zulassen: Sie können SSH-Zugriff für den Root-Benutzer zulassen. Diese Option ist standardmäßig ausgeschaltet, da sie zu einem erhöhten Sicherheitsrisiko führt. Wenn diese Option aktiviert ist, kann sich der Root-Benutzer über seinen öffentlichen Schlüssel anmelden. Laden Sie den/die öffentlichen Schlüssel für den Root-Benutzer in das Feld *Autorisierte Schlüssel für Root* hoch.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Shell-Benutzerkennwörter

Geben Sie Kennwörter für die Standard-Zugangsberechtigten `root` und `loginuser` ein. Um das Kennwort für nur eines dieser beiden Konten zu ändern, lassen Sie die beiden Eingabefelder für das andere Konto einfach frei.

Hinweis – Um SSH-Shell-Zugriff zu ermöglichen, müssen zuerst die Kennwörter gesetzt sein. Darüber hinaus können Sie nur Kennwörter vergeben, die den Sicherheitseinstellungen entsprechen, die Sie auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Erweitert* konfiguriert haben. Mit anderen Worten, wenn Sie die Verwendung von komplexen Kennwörtern ausgewählt haben, können Sie hier nur Kennwörter eingeben, die diesen Sicherheitsanforderungen entsprechen.

Lausch-Port für SSH-Daemon

Mit dieser Option können Sie den TCP-Port für das SSH-Protokoll ändern. Der Standard-SSH-Port `22` ist voreingestellt. Um den Port zu ändern, geben Sie einen geeigneten Wert zwischen `1024` und `65535` in das Feld *Portnummer* ein und klicken Sie auf *Übernehmen*.

4.1.5 Scan-Einstellungen

Einstellungen für Antiviren-Mechanismus

Wählen Sie den Antiviren-Mechanismus, der in allen Einzelscan-Konfigurationen des WebAdmin verwendet werden soll. In Zweifachscan-Konfigurationen werden beide Antiviren-Mechanismen verwendet. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Optionen von Advanced Threat Protection

Wählen Sie die Option „Verdächtige Inhalte zur Analyse an SophosLabs senden", um den Schutz zu verbessern. SophosLabs umfasst eine Cloud-basierte Sandbox, in der das Verhalten von potenzieller Schadsoftware automatisch überwacht und analysiert werden kann. Das trägt zu einem noch besseren Schutz Ihrer UTM durch eine schnellere Bereitstellung von Updates bei. Durch eine Deaktivierung dieser Funktion kann sich die Durchführung von Abwehrmaßnahmen etwas verzögern.

Die Übermittlung erfolgt über einen sicheren Kanal und die Handhabung gemäß der SophosLabs-Richtlinie zur Informationssicherheit.

4.1.6 Zurücksetzung

Mit den Optionen auf der Registerkarte *Zurücksetzung* können Sie die Kennwörter der Shell-Benutzer löschen. Darüber hinaus können Sie die Werkszurücksetzung ausführen und die System-ID der UTM zurücksetzen.

Systemkennwörter zurücksetzen

Das Ausführen der Funktion *Systemkennwörter jetzt zurücksetzen* setzt die Kennwörter der folgenden Benutzer zurück:

- root (Shell-Benutzer)
- loginuser (Shell-Benutzer)
- admin (vordefiniertes Benutzerkonto des Administrators)

Um das Gerät nach dem Zurücksetzen der Kennwörter herunterzufahren, wählen Sie die Option *System anschließend herunterfahren*.

Sicherheitshinweis – Der nächsten Person, die sich mit dem WebAdmin verbindet, wird das Dialogfenster *Admin-Kennworteinrichtung* angezeigt. Deshalb sollten Sie sich nach einer Kennwortzurücksetzung sofort abmelden, die Webseite neu laden und ein neues Administratorkennwort setzen.

Des Weiteren wird der Shell-Zugriff nicht mehr möglich sein, bis Sie neue Shell-Kennwörter auf der Registerkarte *Verwaltung* > *Systemeinstellungen* > *Shell-Zugriff* angeben.

Werkszurücksetzung

Die Funktion *Werkszurücksetzung jetzt ausführen* setzt das System in den Auslieferungszustand zurück. Die folgenden Daten werden dabei gelöscht:

- Systemkonfiguration
- Webfilter-Cache
- Protokoll- und Berichtsdaten
- Datenbanken
- Up2Date-Pakete
- Lizenzen
- Kennwörter
- Hochverfügbarkeitsstatus

Die Versionsnummer der Sophos UTM-Software bleibt hingegen unverändert – alle installierten Firmware- und Pattern-Aktualisierungen werden beibehalten.

Hinweis – Sophos UTM wird ausgeschaltet, nachdem Sie eine Werkszurücksetzung veranlasst haben.

UTM-ID-Zurücksetzung

Mit der Funktion *UTM-ID jetzt zurücksetzen* setzen Sie die System-ID der UTM auf einen neuen, zufälligen Wert zurück. Dies ist beispielsweise dann relevant, wenn Sie Endpoint-Protection aktivieren. Jede UTM mit aktivierter Endpoint-Protection identifiziert sich selbst in Sophos LiveConnect mit ihrer eindeutigen System-ID. Wenn Sie beispielsweise eine virtuelle UTM, die Endpoint-Protection verwendet, klonen und möchten, dass der Klon diese Funktion ebenfalls verwendet, müssen Sie die UTM-System-ID des geklonten Systems zurücksetzen, damit Sie

es anschließend anhand der neuen System-ID identifizieren können. Bei Zurücksetzen wird Endpoint-Protection ausgeschaltet, falls die Funktion eingeschaltet war.

Hinweis – Endpoints sind an die UTM mithilfe der UTM-System-ID angebunden. Wenn Sie die UTM-System-ID zurücksetzen und keine andere UTM auf der alten UTM-ID lauscht, müssen Sie die Endpoints neu installieren.

Hinweis – Wenn eine UTM mit SophosUTM Manager verbunden wird und Sie die UTM-System-ID zurücksetzen, wird die UTM als neues Gerät verbunden. Bei Bedarf können Sie die beiden Geräte zusammenführen.

4.2 WebAdmin-Einstellungen

Im Menü *Verwaltung* > *WebAdmin-Einstellungen* werden die grundlegenden Einstellungen für WebAdmin vorgenommen, wie zum Beispiel die Zugriffskontrolle, der TCP-Port, Benutzereinstellungen und die WebAdmin-Sprache.

4.2.1 Allgemein

Auf der Registerkarte *WebAdmin-Einstellungen* > *Allgemein* wird die Konfiguration der WebAdmin-Sprache und der grundlegenden Zugriffseinstellungen vorgenommen.

WebAdmin-Sprache

Wählen Sie die Sprache des WebAdmin. Die ausgewählte Sprache wird auch für einige Ausgaben des WebAdmin verwendet, z. B. E-Mail-Benachrichtigungen oder den Gesamtbericht. Beachten Sie, dass diese Einstellung global ist und alle Benutzer betrifft. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Nach dem Ändern der Sprache sollten Sie den Browser-Cache leeren, um sicherzustellen, dass alle Texte in der korrekten Sprache angezeigt werden.

WebAdmin-Zugriffskonfiguration

Hier können Sie konfigurieren, welche Benutzer und/oder Netzwerke Zugriff auf den WebAdmin haben sollen.

Zugelassene Administratoren: Sophos UTM kann von mehreren Administratoren gleichzeitig verwaltet werden. Im Feld *Zugelassene Administratoren* können Sie angeben, welche

Benutzer oder Benutzergruppen unbeschränkten Lese- und Schreibzugriff auf WebAdmin haben dürfen. Standardmäßig ist dies die Gruppe der *SuperAdmins*. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

Zugelassene Netzwerke: Im Feld *Zugelassene Netzwerke* können Sie festlegen, aus welchen Netzwerken Zugriff auf WebAdmin möglich sein soll. Für eine reibungslose Installation von UTM ist standardmäßig `Any` eingestellt. Das bedeutet, dass von überall her auf den WebAdmin zugegriffen werden darf. Ändern Sie diese Einstellung so schnell wie möglich auf Ihre internen Netze. Die sicherste Lösung ist jedoch, den Zugriff auf die UTM über HTTPS auf nur einen Administrator-PC zu beschränken. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Zugriffsverkehr protokollieren: Wenn Sie alle Aktivitäten des WebAdmin-Zugriffs in der Firewall-Protokolldatei aufgeführt haben möchten, wählen Sie die Option *Zugriffsverkehr protokollieren*.

4.2.2 Zugriffskontrolle

Auf der Registerkarte *WebAdmin-Einstellungen > Zugriffskontrolle* können Sie WebAdmin-Rollen für bestimmte Benutzer anlegen. Das ermöglicht eine sehr detaillierte Definition der Berechtigungen, die ein Benutzer im WebAdmin haben kann.

Es sind zwei Benutzerrollen vordefiniert:

Auditor: Benutzer mit dieser Rolle können Protokoll- und Berichtsdaten einsehen.

Readonly: Benutzer mit dieser Rolle können alles in WebAdmin anzeigen, aber nichts bearbeiten, anlegen oder löschen.

Um Benutzern oder Gruppen eine dieser Rollen zuzuweisen, klicken Sie auf die Schaltfläche *Bearbeiten* und fügen Sie die entsprechenden Benutzer oder Gruppen zum Feld *Mitglieder* hinzu.

Entsprechend Ihrer Sicherheitsrichtlinien können Sie weitere Rollen anlegen. Gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zugriffskontrolle* auf *Neue Rolle*.**
   Das Dialogfeld *Rolle anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Definition ein.

Mitglieder: Fügen Sie Benutzer und Gruppen, die diese Rolle besitzen sollen, zu diesem Feld hinzu oder wählen Sie sie aus.Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

Nur Leserechte gewähren (optional): Wählen Sie diese Option, um den Mitgliedern für alle Bereiche von WebAdmin Leserechte zu geben.

Rechte: Dieses Feld enthält die verschiedenen Berechtigungsstufen für die verschiedenen Funktionen von WebAdmin: Auditor und Manager. Ein Manager hat alle Administrationsrechte für die jeweiligen Funktionen, wohingegen ein Auditor nur Leserechte hat. Sie können eine oder mehrere Berechtigungen auswählen, indem Sie das entsprechende Auswahlkästchen vor einer Berechtigung markieren.
Beispiel: Sie können dem Benutzer Hans Mustermann Manager-Rechte für Email Protection gewähren und zusätzlich das Auswahlfeld *Nur Leserechte gewähren* markieren. Er wäre dann in der Lage, Änderungen im Bereich Email Protection durchzuführen, und könnte alle anderen Bereiche von WebAdmin einsehen, ohne dort etwas ändern zu können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

Um eine Rolle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen. Beachten Sie, dass die *Auditor*- und die *Readonly*-Rollen nicht gelöscht werden können.

4.2.3 HTTPS-Zertifikat

Auf der Registerkarte *Verwaltung > WebAdmin-Einstellungen > HTTPS-Zertifikat* können Sie das WebAdmin-CA-Zertifikat in Ihren Browser importieren, neu generieren oder ein signiertes Zertifikat für WebAdmin und das Benutzerportal auswählen.

Während der Erstkonfiguration des WebAdmin-Zugriffs wurde automatisch ein lokales CA-Zertifikat auf UTM erzeugt. Der öffentliche Schlüssel dieses CA-Zertifikats kann in Ihrem Browser installiert werden, um den Sicherheitshinweis während der Anmeldung am WebAdmin zu vermeiden.

Um das CA-Zertifikat zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *HTTPS-Zertifikat* auf *CA-Zertifikat importieren*.**
   Der öffentliche Schlüssel des CA-Zertifikats wird exportiert.

   Sie können das Zertifikat entweder auf der Festplatte abspeichern oder es in Ihrem Browser installieren.

2. **Installieren Sie das Zertifikat** (optional).
   Der Browser öffnet ein Dialogfenster, über das Sie das Zertifikat sofort installieren können.

Hinweis – Beachten Sie, dass das Zertifikat aufgrund von unterschiedlichen Systemzeiten und Zeitzonen möglicherweise nicht sofort nach der Erzeugung gültig ist. Viele Browser geben in diesem Fall die Meldung aus, dass das Zertifikat abgelaufen sei. Diese Meldung ist nicht richtig. Aber das Zertifikat wird nach spätestens 24 Stunden gültig und bleibt dies für einen Zeitraum von 27 Jahren.

WebAdmin-Zertifikat neu erstellen

Das WebAdmin-Zertifikat bezieht sich auf den Hostnamen, den Sie während der ersten Anmeldung angegeben haben. Wenn sich der Hostname in der Zwischenzeit geändert hat, wird im Browser eine entsprechende Sicherheitswarnung angezeigt. Um dies zu vermeiden, können Sie ein neues Server-Zertifikat erzeugen, das den neuen Hostnamen berücksichtigt. Geben Sie zu diesem Zweck den gewünschten Hostnamen an und klicken Sie auf *Übernehmen*. Um im WebAdmin weiterarbeiten zu können, müssen Sie wahrscheinlich – aufgrund der Änderung des Zertifikats – die Seite über Ihren Browser neu laden, das neue Zertifikat akzeptieren und sich am WebAdmin neu anmelden.

WebAdmin-/Benutzerportal-Zertifikat auswählen

Wenn Sie das CA-Zertifikat nicht importieren wollen, sondern stattdessen Ihr eigenes signiertes Zertifikat für den WebAdmin und das Benutzerportal verwenden wollen, können Sie es hier auswählen. Wenn das Zertifikat jedoch in die Auswahlliste aufgenommen werden soll, müssen Sie es erst über die Registerkarte *Fernzugriff > Zertifikatverwaltung > Zertifikate* im Format PKCS#12 hochladen, welches das Zertifikat, seine CA und seinen privaten Schlüssel enthält. Um das hochgeladene Zertifikat zu verwenden, wählen Sie es in der Auswahlliste *Zertifikate* aus und klicken auf *Übernehmen*.

4.2.4 Benutzereinstellungen

Auf der Registerkarte *Verwaltung* > *WebAdmin-Einstellungen* > *Benutzereinstellungen* können Sie einige Benutzereinstellungen für den jeweils angemeldeten Benutzer vornehmen, wie zum Beispiel globale Tastaturkürzel und die Anzahl von Elementen pro Seite bei längeren Tabellen oder Listen.

Konfiguration der WebAdmin-Tastaturkürzel

Hier können Sie Tastaturkürzel festlegen, um Objektlisten, die für viele Konfigurationen verwendet werden, zu öffnen und zu schließen (weitere Informationen zu Objektlisten finden Sie unter *WebAdmin* > *Objektlisten*) oder um den Mauszeiger in das Suchfeld zu setzen (siehe auch *WebAdmin* > *WebAdmin-Menü*). Verwenden Sie die Auswahlliste, um eine andere Umschalttaste auszuwählen, und das Textfeld, um ein anderes Zeichen einzugeben. Sie können Tastaturkürzel auch ausschalten, indem Sie *Aus* aus der Auswahlliste wählen.

Wenn Sie die ursprünglichen Tastaturkürzel wiederherstellen wollen, klicken Sie auf die Schaltfläche *Auf Standard zurücksetzen*. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Optionen für Tabellen-Seitenumbruch

Hier können Sie global den Tabellenseiten-Umbruch festlegen, d. h. wie viele Elemente pro Seite angezeigt werden. Klicken Sie auf die Auswahlliste und wählen Sie einen Wert. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

WebAdmin-Browsertitel anpassen

Hier können Sie den Titel des WebAdmin-Registers/-Fensters in Ihrem Browser ändern. Sie können Klartext eingeben oder die folgenden Variablen verwenden:

- %h: Hostname
- %u: Benutzername
- %i: Remote-IP-Adresse

Die Standardeinstellung lautet `WebAdmin - User %u - Device %h`, was sich beispielsweise in den Titel *WebAdmin - User admin - Device mein_gateway.beispiel.de* umsetzen lässt. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

4.2.5 Erweitert

WebAdmin-Abmeldung bei Zeitüberschreitung

Abmelden nach: In diesem Textfeld können Sie angeben (in Sekunden), wie lange eine WebAdmin-Sitzung inaktiv sein darf, bevor sich der Administrator neu anmelden muss. Standardmäßig sind 1.800 Sekunden voreingestellt. Sie können Werte von 60 bis 86.400 Sekunden eingeben.

Abmeldung im Dashboard: Beachten Sie, dass die automatische Abmeldung aktiviert ist, wenn die *Dashboard*-Seite im WebAdmin geöffnet ist. Indem Sie diese Option auswählen, können Sie die automatische Abmeldung für das Dashboard deaktivieren.

WebAdmin-TCP-Port

Standardmäßig erreicht man den WebAdmin über TCP-Port `4444`.Im Textfeld *TCP-Port* können Sie entweder `443` oder einen Wert zwischen `1024` und `65535` eintragen. Allerdings sind einige Ports bereits von anderen Diensten belegt. Insbesondere können Sie niemals den Port `10443`, den Port des Benutzerportals oder den Port für den SSL-Fernzugriff verwenden. Beachten Sie, dass Sie die Portnummer in der IP-Adresse angeben müssen (durch einen Doppelpunkt abgetrennt), wenn Sie auf WebAdmin zugreifen möchten, z. B. `https://192.168.0.1:4444`

Nutzungsbedingungen

Ihre Unternehmensrichtlinien sehen es ggf. vor, dass Benutzer die Nutzungsbedingungen akzeptieren müssen, bevor sie auf den WebAdmin zugreifen können. Aktivieren Sie das Auswahlkästchen *Nutzungsbedingungen nach der Anmeldung anzeigen*, um zu erzwingen, dass die Benutzer die Nutzungsbedingungen bei jedem Zugriff auf WebAdmin akzeptieren. Die Nutzungsbedingungen werden den Benutzern unmittelbar nach der Anmeldung angezeigt. Wenn sie sie nicht akzeptieren, werden sie wieder abgemeldet.

Sie können den Text der Nutzungsbedingungen nach Ihren Bedürfnissen anpassen.Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Sophos Adaptive Learning

Sie können zur Verbesserung von Sophos UTM beitragen, indem Sie der Übertragung Ihrer aktuellen Konfigurationsdaten in anonymer Form sowie von Informationen über gefundene Viren oder anonyme Anwendungsprofile an Sophos zustimmen. Informationen dieser Art können nicht zu Ihnen zurückverfolgt werden. Keine benutzerspezifischen Informationen werden

erfasst, also keine Benutzer- oder Objektnamen, keine Kommentare oder andere persönliche Informationen. Es werden jedoch URLs übermittelt, für die ein Virus gefunden wurde, falls das Antiviren-Scanning des Webfilters aktiv ist.

Die Informationen werden verschlüsselt und mittels SSL an Sophos übertragen. Die empfangenen Daten werden zusammengefasst gespeichert und den Softwareentwicklern von Sophos zur Verfügung gestellt, sodass sie bei der Entwicklung fundierte Entscheidungen treffen und zukünftige Versionen von Sophos UTM verbessern können.

Anonyme Telemetriedaten senden Bei Aktivierung erfasst UTM folgende Daten:

- Konfigurations- und Nutzungsdaten: Das System sendet einmal pro Woche die folgenden Daten an die Server von Sophos.
  - Hardware- und Lizenzdaten (nicht den Eigentümer), z. B.:

    ```
    processor Intel(R) Core(TM)2 Duo CPU E8200 @ 2.66GHz
    memory 512MiB System Memory
    eth0 network 82545EM Gigabit Ethernet Controller
    id:UTM
    version: 9.000000
    type: virtual
    license: standard
    mode: standalone
    active_ips: 2
    system_id: 58174596-276f-39b8-854b-ffa1886e3c6c
    ```

    Die System-ID identifiziert UTM nur insofern, dass Systemdaten nicht versehentlich doppelt erfasst werden, z. B. nach einer Neuinstallation.
  - Verwendete Funktionen (nur ob aktiviert oder deaktiviert), z. B.:

    ```
    main->backup->status: 1
    main->ha->status: off
    ```
  - Anzahl der konfigurierten Objekte, z. B.:

    ```
    objects->interface->ethernet: 2
    objects->http->profile: 5
    ```
  - CPU-, Speicher- und SWAP-Nutzungswerte in Prozent über die letzten sieben Tage
- Virendaten: Das System schreibt die folgenden Daten in eine Datei, die automatisch alle

15 Minuten auf den Sophos-Server hochgeladen wird.

  - Informationen über Viren, die von Web Protection gefunden wurden, z. B. Name der Bedrohung, MIME-Typ, URL der Anfrage oder Dateigröße.

- Intrusion-Prevention-Daten: Das IPS-Protokoll wird einmal pro Minute auf neue Warnungen (Alerts) überprüft. Sobald eine neue Warnung gefunden wird, werden sofort die folgenden Daten an Sophos gesendet:

  - Informationen über die Warnung, beispielsweise die Snort-Regel-ID und der Zeitstempel.
  - Hardware- und Lizenzdaten (nicht den Eigentümer), z. B. Anzahl Prozessoren und Prozessorlast, Speicherkapazität und Speichernutzung, SWAP-Zuweisung und SWAP-Nutzung, System-ID, Engine- und Patternversion.

    Die Daten werden alle 24 Stunden gesendet.

- Daten von Advanced Threat Protection: Das System generiert und sendet die Daten von Advanced Threat Protection alle 30 Minuten.

  - Erfasste Daten: System-ID, Zeitstempel, Sophos Bedrohungsname, Quell-IP, Zielhost, Erkennungskomponente, Erkennungsdetails, Anzahl der Bedrohungen, Regel-ID.

Anonyme Telemetriedaten zur Anwendungsgenauigkeit senden: Sie können uns dabei helfen, die Erkennungs- und Klassifizierungsfunktionen im Bereich Netzwerksichtbarkeit und Application Control zu verbessern, indem Sie am Sophos UTM AppAccuracy-Programm teilnehmen. Bei Aktivierung erfasst das System Daten in Form anonymer Anwendungsprofile und sendet diese an das Forschungsteam von Sophos. Dort werden die Profile genutzt, um nicht klassifizierte Anwendungen zu identifizieren und die Netzwerksichtbarkeits- und Application-Control-Bibliothek zu verbessern und zu erweitern.

4.3 Lizenzen

Die Verfügbarkeit von bestimmten Funktionen auf Sophos UTM wird über Lizenzen und Abonnements geregelt, d. h. die Lizenzen und Abonnements, die Sie mit der UTM erworben haben, ermöglichen Ihnen die Nutzung bestimmter Funktionen, anderer jedoch nicht.

4.3.1 Erwerb einer Lizenz

Sophos UTMwird standardmäßig mit einer 30-Tage-Testlizenz ausgeliefert, mit der Sie alle Leistungsmerkmale und Funktionen uneingeschränkt nutzen können. Nach Ablauf müssen Sie eine gültige Lizenz installieren, um die Sophos UTM weiter nutzen zu können. Alle Lizenzen (einschließlich kostenloser Home-Use-Lizenzen) werden im MyUTM-Portal angelegt.

Nach dem Kauf einer UTM-Lizenz erhalten Sie per E-Mail Ihre Aktivierungsschlüssel. Diese Schlüssel benötigen Sie, um die eigentliche Lizenz zu generieren bzw. eine bereits bestehende Lizenz zu aktualisieren. Um eine Lizenz zu aktivieren, melden Sie sich im MyUTM-Portal an und gehen Sie zur Lizenzverwaltungsseite. Oben auf der Seite befindet sich ein Formular, wo Sie den Aktivierungsschlüssel aus der E-Mail kopieren und einfügen können. Weitere Informationen finden Sie im MyUTM-Benutzerhandbuch.

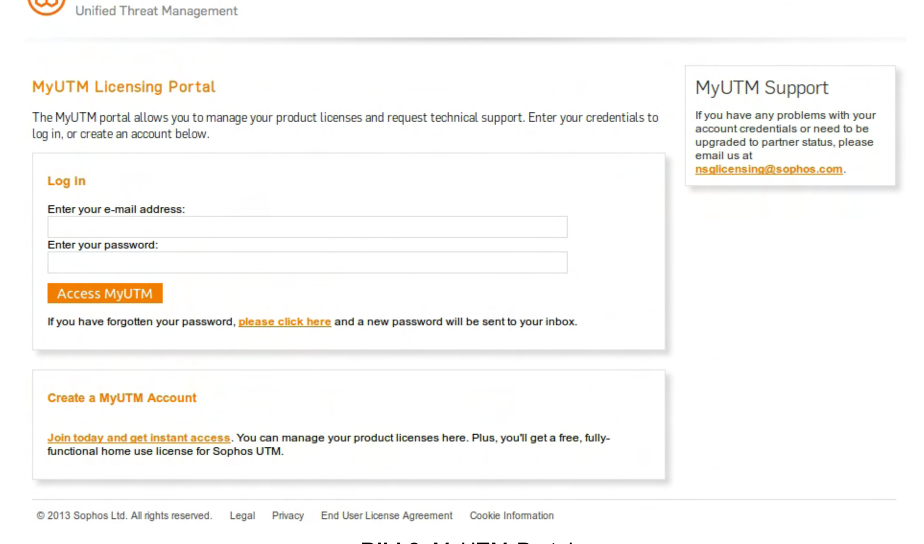


Bild 8 MyUTM-Portal

Ein neues Formular wird angezeigt, in das Sie sowohl Informationen zu Ihrem Vertriebspartner als auch Ihre eigenen Kontaktdaten eintragen können. Das Portal versucht, so viele Felder wie möglich vorauszufüllen. Außerdem erfasst Sophos ggf. die Hardware-Seriennummer der UTM. Nachdem Sie das Formular abgeschickt haben, wird Ihre Lizenz erzeugt und Sie werden auf die Lizenz-Detailseite weitergeleitet, von der aus Sie die Lizenz herunterladen können.

Um die Lizenz verwenden zu können, müssen Sie die erzeugte Lizenz-Datei herunterladen und sich dann an Ihrer WebAdmin-Installation anmelden. Öffnen Sie in WebAdmin die Registerkarte *Verwaltung > Lizenzen > Installation* und verwenden Sie die Upload-Funktion, um die Lizenzdatei auf Ihrer Festplatte zu finden. Laden Sie die Lizenzdatei hoch. Danach wird der WebAdmin sie einlesen, um alle Abonnements und anderen Einstellungen zu aktivieren, die in der Lizenzdatei vorgesehen sind.

Hinweis – Der Aktivierungsschlüssel, den Sie per E-Mail erhalten haben, kann nicht in den WebAdmin importiert werden. Dieser Schlüssel dient lediglich zur Aktivierung Ihrer Lizenz.Nur die Lizenz-Datei kann in die UTM importiert werden.

4.3.2 Lizenzmodell

Das modulare Lizenzmodell von Sophos ist äußerst flexibel. Zunächst gibt es eine Basislizenz, die grundlegende Funktionen kostenlos bereitstellt (siehe Tabelle unten). Des Weiteren gibt es sechs weitere Abonnements:

- Network Protection
- Web Protection
- Email Protection
- Endpoint Protection
- Wireless Protection
- Webserver Protection

Diese Abonnements können Ihren Anforderungen entsprechend einzeln oder in Kombination erworben werden. Die FullGuard-Lizenz enthält alle Abonnements. Jedes der Abonnements aktiviert bestimmte Funktionen des Produkts. Die untenstehende Tabelle zeigt eine Übersicht darüber, welche Funktionen durch welches Abonnement freigeschaltet werden.

Funktion	Basis-lizenz	Netz-werk	Web	E-Mail	End-point	Wire-less	Webser-ver
Verwaltung (Backups, Benach-richtigungen, SNMP, SUM, ...)	✓						

Funktion	Basis-lizenz	Netz-werk	Web	E-Mail	End-point	Wire-less	Webser-ver
Lokale Authen-tifizierung (Benut-zer, Gruppen)	✓						
Grundlegende Netz-werkfunktionen (Statisches Rou-ting, DHCP, DNS, Auto-QoS, NTP, ...)	✓						
Firewall/NAT (DNAT, SNAT, ...)	✓						
PPTP- & L2TP-Fernzugriff	✓						
Lokale Pro-tokollierung, Stan-dardberichte	✓						
Intrusion Pre-vention (IPS, dt. Angriffsschutz) (Patterns, DoS, Flood, Portscan ...)		✓					
IPsec- & SSL-Site-to-Site-VPN, IPsec- & SSL-Fernzugriff		✓					

Funktion	**Basislizenz**	**Netzwerk**	**Web**	**E-Mail**	**Endpoint**	**Wireless**	**Webserver**
Erweiterte Netzwerkfunktionen (Linkbündelung, Uplink-Ausgleich, Richtlinien-Routing, OSPF, Multicast, angepasstes QoS, Serverlastausgleich, Generischer Proxy ...)		✓	(✓)	(✓)			
Benutzerportal		✓	✓	✓			
High Availabilty (Hochverfügbarkeit)		✓	✓	✓			
Entfernte Authentifizierung (AD, eDir, RADIUS, ...)		✓	✓	✓			
Ausgelagerte Protokollierung, erweiterte Berichte (Archivierung, Konfiguration)		✓	✓	✓			
Basis-Webfilter & FTP-Proxy			✓				
Web- & FTP-Schadsoftware-Filterung			✓				
Application Control			✓				

Funktion	Basis-lizenz	Netz-werk	Web	E-Mail	End-point	Wire-less	Webser-ver
Basis-SMTP-Proxy, Quarantänebericht, Mail-Manager				✓			
SMTP- & POP3-Schadsoftware-Filterung				✓			
Endpoint Protection, Antivirus					✓		
Endpoint Protection, Device Control					✓		
Wireless Protection						✓	
Webserver Protection							✓

Es gibt auch ein BasicGuard-Abonnement, das für das UTM-Appliance-Model 100 verfügbar ist, und eine eigene Untermenge der oben genannten Funktionen bietet (Mehr Informationen finden Sie auf der Produkt-Webseite).

UTMs können auch vom Sophos UTM Manager (SUM) verwaltet und lizenziert sein.In diesem Fall übergibt SUM die MSP-Lizenz (Managed Service Provider) an die UTM und die Registerkarte *Installation* ist inaktiv. Abonnements können dann nur von Ihrem SUM-Dienstleister aktiviert werden.

Für genauere Informationen zu Abonnements und ihrem Funktionsumfang wenden Sie sich bitte an Ihren zertifizierten UTM-Partner oder die Sophos UTMWebseite.

Wenn bestimmte Abonnements nicht erworben wurden, sind die entsprechenden Registerkarten im WebAdmin inaktiv. Über den Registerkarten wird eine Warnmeldung zur Lizenzierung angezeigt.

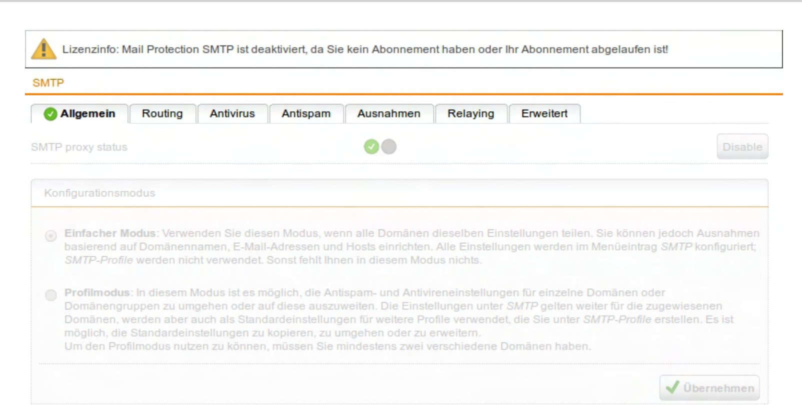


Bild 9 Lizenzen: Abonnement-Warnhinweis

Up2Dates

Jedes Abonnement aktiviert die vollständige Unterstützung automatischer Updates, das bedeutet, dass Sie automatisch über neue Firmware-Updates informiert werden. Darüber hinaus können Firmware- und Pattern-Updates automatisch heruntergeladen (und installiert) werden.

Eine Basislizenz ohne Abonnement unterstützt automatische Updates nur eingeschränkt: Lediglich Pattern-Updates, wie z. B. Aktualisierungen der Onlinehilfe, werden weiterhin automatisch heruntergeladen und installiert. Sie werden jedoch nicht über verfügbare Firmware-Updates informiert, und die Firmware-Updates müssen manuell heruntergeladen werden. Die Verfügbarkeit neuer Firmware-Updates wird im Sophos UTMUp2Date-Blog bekanntgegeben

Support und Wartung

Mit der Basislizenz können Sie den *Web-Support* nutzen. Sie können das Sophos UTMSupport-Forum und die SophosKnowledgebase nutzen.

Sobald Sie eines der Abonnements erwerben, werden Sie automatisch auf *Standard-Support* umgestellt. Bei dieser Supportstufe können Sie zusätzlich einen Supportfall im MyUTM-Portal anlegen oder Ihren zertifizierten UTM-Partner kontaktieren.

Darüber hinaus gibt es die Möglichkeit, einen *Premium-Support*-Vertrag abzuschließen. Dieser bietet Ihnen rund um die Uhr Support durch einen UTM-Engineer als Ansprechpartner.

4.3.3 Übersicht

Die *Die Registerkarte Lizenzen* > *Übersicht* zeigt detaillierte Informationen zu Ihrer Lizenz und besteht aus mehreren Abschnitten:

- **Basislizenz:** Grundlegende Lizenzparameter wie ID, Registrierungsdatum oder Typ.
- **Network Protection, Email Protection, Web Protection, Webserver Protection, Wireless Protection, Endpoint AntiVirus, BasicGuard:** Diese Abschnitte geben Informationen zu den Abonnements, beispielsweise ob diese erworben wurden und daher aktiviert sind, ihr Ablaufdatum und eine Kurzbeschreibung der Funktionen, die sie bieten.

  Hinweis – Wenn Sie die MSP-Lizenz nutzen, werden keine Ablaufdaten angezeigt, da die Lizenzen vom Sophos UTM Manager (SUM) verwaltet werden. Herkömmliche Schlüssel und Abonnements sind durch das SUM-MSP-System ersetzt.Informationen über den verwaltenden SUM finden Sie unter *Zentrale Verwaltung* > *Sophos UTM Manager*.

- **Support-Dienste:** Supportstufe sowie Gültigkeitszeitraum

4.3.4 Installation

Auf der *Registerkarte Verwaltung* > *Lizenzen* > *Installation* können Sie neue Lizenzen hochladen und installieren.

Hinweis – Wenn Sie die MSP-Lizenz nutzen, ist die Registerkarte deaktiviert, da Lizenzen durch den Sophos UTM Manager (SUM) verwaltet werden. Neue Lizenzen können durch Ihren SUM-Dienstleister installiert werden.Informationen über den verwaltenden SUM finden Sie unter *Zentrale Verwaltung* > *Sophos UTM Manager*.

Um eine Lizenz zu installieren, gehen Sie folgendermaßen vor:

1. **Öffnen Sie das Dialogfenster *Datei hochladen*.**
   Klicken Sie dazu auf das Ordnersymbol neben dem Eingabefeld *Lizenzdatei*.

   Das Dialogfenster *Datei hochladen* öffnet sich.

2. **Wählen Sie die Lizenzdatei aus.**
   Wechseln Sie in das Verzeichnis, in dem sich Ihre Lizenzdatei befindet.

   Wählen Sie die Lizenzdatei aus, die Sie installieren wollen.

3. **Klicken Sie auf *Hochladen starten*.**
   Ihre Lizenzdatei wird hochgeladen.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Lizenz wird nun installiert. Beachten Sie, dass die neue Lizenz automatisch eine bereits installierte Lizenz ersetzt.

   Die Installation der Lizenz dauert ca. 60 Sekunden.

4.3.5 Aktive IP-Adressen

Die kostenlose Sophos-UTM-Manager-Lizenz ermöglicht eine unbegrenzte Anzahl an IP-Adressen.

Falls Sie eine Lizenz erworben haben, die nicht uneingeschränkt viele Benutzer (IP-Adressen) erlaubt, zeigt Ihnen diese Registerkarte Informationen über die zulässige Anzahl an IP-Adressen, die von Ihrer Lizenz abgedeckt werden. IP-Adressen, die den Umfang Ihrer Lizenz überschreiten, werden gesondert aufgelistet. Falls Sie die zulässige Grenze überschritten haben, erhalten Sie regelmäßig eine E-Mail-Benachrichtigung.

Hinweis – IP-Adressen, die über einen Zeitraum von sieben Tagen inaktiv waren, werden nicht mehr eingerechnet.

4.4 Up2Date

Das Menü *Verwaltung > Up2Date* ermöglicht die Konfiguration des Aktualisierungsdienstes von Sophos UTM. Regelmäßige Aktualisierungen sorgen dafür, dass die UTM stets über die neuesten Fehlerkorrekturen, Produktverbesserungen und aktuellen Virensignaturen verfügt. Jede Aktualisierung wird von Sophos digital signiert – unsignierte oder gefälschte Aktualisierungen können so erkannt und Installationen von gefälschten Aktualisierungen verhindert werden.

Es gibt zwei Arten von Software-Aktualisierungen:

- **Firmware-Aktualisierungen:** Firmware-Aktualisierungen enthalten Fehlerkorrekturen und Produktverbesserungen für Sophos UTM-Software.
- **Pattern-Aktualisierungen:** Pattern-Aktualisierungen halten Virus-, Spam- und Angriffschutz-Signaturen sowie die Onlinehilfe auf dem neuesten Stand.

Um Up2Date-Pakete herunterzuladen, öffnet die UTM eine TCP-Verbindung zu den Aktualisierungsservern auf Port `443`. Hierfür müssen vom Administrator keinerlei Anpassungen vorgenommen werden. Falls Sie jedoch eine übergeordnete Firewall verwenden, so müssen Sie auf dieser die Kommunikation über TCP-Port `443` zu den Aktualisierungsservern explizit erlauben.

4.4.1 Übersicht

Die Registerkarte *Verwaltung* > *Up2Date* > *Übersicht* gibt Ihnen einen schnellen Überblick darüber, ob Ihr System auf dem neuesten Stand ist. Von hier aus können Sie neue Firmware- und Pattern-Aktualisierungen installieren.

Up2Date-Fortschritt

Dieser Bereich ist nur sichtbar, wenn Sie einen Installationsvorgang angestoßen haben. Klicken Sie auf die Schaltfläche *Up2Date-Fortschritt in neuem Fenster anzeigen*, um den Aktualisierungsfortschritt zu verfolgen. Wenn Ihr Browser Pop-up-Fenster nicht unterdrückt, wird ein neues Fenster geöffnet, das den Aktualisierungsfortschritt anzeigt. Andernfalls müssen Sie Pop-up-Fenster zunächst explizit erlauben.

Hinweis – Bevor ein Installationsvorgang gestartet wird, wird ein Backup an den/die Standardempfänger für Backups versendet.

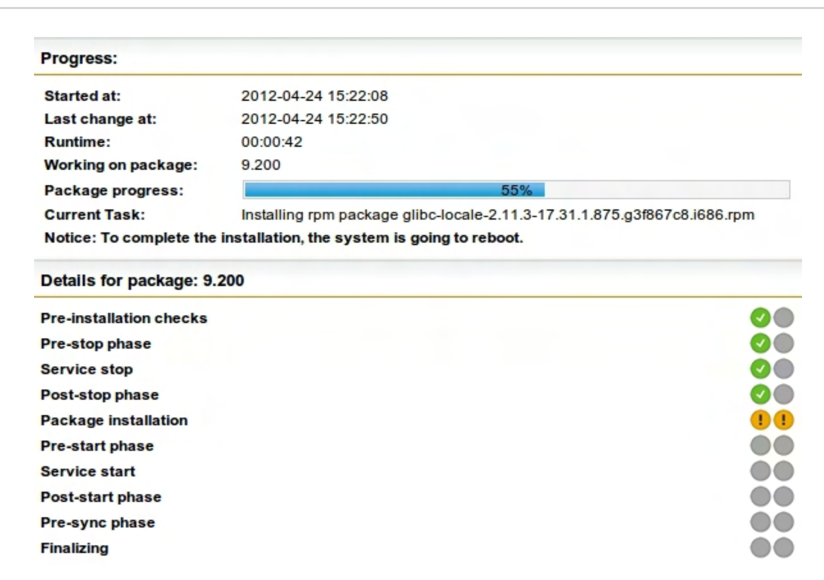


Bild 10 Up2Date: Fortschrittsfenster

Firmware

Im Abschnitt *Firmware* sehen Sie die aktuell installierte Firmware-Version. Wenn ein Aktualisierungspaket verfügbar ist, wird eine Schaltfläche *Jetzt auf neueste Version aktualisieren* angezeigt. Zusätzlich wird eine Nachricht im Abschnitt *Verfügbare Firmware-Up2Dates* angezeigt. Sie können von hier aus die neueste Aktualisierung direkt herunterladen und installieren. Sobald Sie *Jetzt auf neueste Version aktualisieren* angeklickt haben, können Sie den Aktualisierungsfortschritt in einem neuen Fenster verfolgen. Klicken Sie dazu auf das *Aktualisieren*-Symbol von WebAdmin.

Verfügbare Firmware-Up2Dates

Wenn Sie *Manuell* auf der Registerkarte *Konfiguration* gewählt haben, sehen Sie hier eine Schaltfläche *Jetzt nach Up2Date-Paketen suchen*, mit der Sie Firmware-Up2Date-Pakete manuell herunterladen können. Wenn mehr als ein Up2Date-Paket verfügbar ist, können Sie wählen, welches Sie installieren wollen. Sie können die Schaltfläche *Jetzt auf neueste Version aktualisieren* im Abschnitt *Firmware* verwenden, um die neueste Version zu installieren.
Es gibt außerdem eine Schaltfläche *Planen* für jedes Up2Date, mit der Sie ein genaues Datum und eine genaue Uhrzeit für eine automatische Installation bestimmen können. Um eine geplante Installation zu löschen, klicken Sie auf *Abbrechen*.

Ein Hinweis zu „zwingenden“ Installationen: Es kann Konstellationen geben, in denen Sie die Installation eines Up2Date-Pakets planen, das die vorherige Installation eines älteren Up2Date-Pakets erfordert. Dieses Up2Date-Paket wird automatisch zur Installation eingeplant, und zwar vor dem eigentlichen Up2Date-Paket. Sie können jedoch auch für dieses Paket eine genaue Zeit einplanen, aber Sie können seine Installation nicht verhindern.

Patterns

Im Abschnitt *Patterns* steht die Versionsnummer der aktuell installierten Patterns. Wenn Sie *Manuell* auf der Registerkarte *Konfiguration* gewählt haben, sehen Sie hier eine Schaltfläche *Patterns jetzt aktualisieren*. Mit dieser Schaltfläche können Sie neue verfügbare Patterns herunterladen und installieren.

Hinweis – Die aktuell installierte Patternversion muss nicht mit der neuesten verfügbaren Patternversion übereinstimmen, damit UTM korrekt funktioniert. Eine Abweichung zwischen der aktuell installierten und der aktuell erhältlichen Patternversion kann vorkommen, wenn neue Patterns vorliegen, die jedoch nicht zu dem Gerät passen, das Sie verwenden. Welche Patterns heruntergeladen werden, hängt von Ihren Einstellungen und Ihrer Hardwarekonfiguration ab. Wenn Sie zum Beispiel die Angriffschutzfunktion (IPS) von Sophos UTM nicht verwenden, werden neu verfügbare IPS-Patterns nicht installiert, was den Abstand zwischen installierten und erhältlichen Patternversionen vergrößert.

4.4.2 Konfiguration

Neue Aktualisierungspakete werden standardmäßig automatisch auf die UTM heruntergeladen.

Firmware-Download-Intervall

Diese Option steht standardmäßig auf 15 Minuten, das heißt, dass Sophos UTM alle 15 Minuten nach verfügbaren Firmware-Aktualisierungen sucht. Sophos UTMlädt verfügbare Firmware-Aktualisierungspakete automatisch herunter, ohne sie jedoch zu installieren. Der genaue Zeitpunkt hierfür bewegt sich dabei beliebig in dem angegebenen Zeitraum. Sie können das Intervall auf bis zu *Monatlich* erhöhen oder automatische Firmware-Downloads gänzlich deaktivieren, indem Sie *Manuell* in der Auswahlliste wählen. Wenn Sie *Manuell* wählen, wird eine Schaltfläche *Jetzt nach Up2Date-Paketen suchen* auf der Registerkarte *Übersicht* angezeigt.

Intervall für Pattern-Download und -Installation

Diese Option steht standardmäßig auf 15 Minuten, das heißt, dass Sophos UTM alle 15 Minuten nach verfügbaren Pattern-Aktualisierungen sucht. Sophos UTM lädt verfügbare Pattern-Aktualisierungspakete automatisch herunter und installiert diese. Der genaue Zeitpunkt hierfür bewegt sich dabei beliebig in dem angegebenen Zeitraum. Sie können das Intervall auf bis zu *Monatlich* erhöhen oder automatische Pattern-Downloads und -Installationen gänzlich deaktivieren, indem Sie *Manuell* in der Auswahlliste wählen. Wenn Sie *Manuell* wählen, wird eine Schaltfläche *Patterns jetzt aktualisieren* auf der Registerkarte *Übersicht* angezeigt.

4.4.3 Erweitert

Auf der Registerkarte *Verwaltung* > *Up2Date* > *Erweitert* gibt es weitere Konfigurationsmöglichkeiten für die Aktualisierungsfunktionalität Ihrer UTM, wie die Angabe eines übergeordneten Proxy (engl. parent proxy) oder eines Up2Date-Caches.

> **Hinweis –** Aktualisierungspakete können vom Sophos UTMFTP-Server heruntergeladen werden.

Manuelles Hochladen von Up2Date-Paketen: Wenn Ihre UTM keinen direkten Zugang zum Internet oder einem Up2Date-Zwischenspeicher (engl. Cache) hat, um Aktualisierungspakete herunterzuladen, können Sie diese auch manuell hochladen. Gehen Sie dazu folgendermaßen vor:

1. **Öffnen Sie das Dialogfenster *Datei hochladen*.**
   Klicken Sie auf das Ordnersymbol neben dem Feld *Up2Date-Datei*.

   Das Dialogfeld *Datei hochladen* öffnet sich.

2. **Wählen Sie das Aktualisierungspaket.**
   Klicken Sie im Dialogfenster *Datei hochladen* auf die Schaltfläche *Durchsuchen* und wählen Sie das Aktualisierungspaket aus, das Sie hochladen möchten.

3. **Klicken Sie auf *Hochladen starten*.**
   Das Aktualisierungspaket wird auf die UTM hochgeladen.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Übergeordneter Proxy

Ein übergeordneter Proxy (auch Parent oder Upstream Proxy) wird in Ländern benötigt, in denen der Zugang zum Internet nur über einen staatlich kontrollierten Proxy erlaubt ist. Falls Ihre Sicherheitsbestimmungen die Nutzung eines übergeordneten Proxys erforderlich machen, so können Sie diesen hier durch Angabe einer Hostdefinition und eines Ports konfigurieren.

Übergeordneten Proxy verwenden: Wählen Sie diese Option, um einen übergeordneten Proxy zu verwenden. Wählen Sie den Host aus oder fügen Sie einen Host hinzu und geben Sie den Proxy-Port ein. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort hier ein.

Falls Sie einen übergeordneten Proxy eingerichtet haben, holt sich Sophos UTM die Aktualisierungspakete von diesem Proxy.

4.5 Backup/Wiederherstellen

Mit der Backup-Funktion können Sie die Einstellungen der UTM auf einer lokalen Festplatte sichern. Mit Hilfe der Backup-Datei sind Sie in der Lage, eine erprobte Konfiguration auf neu installierte oder fehlkonfigurierte Systeme zu übertragen.

Legen Sie nach jeder Änderung der Systemeinstellungen eine neue Backup-Datei an. Auf diese Weise haben Sie immer die aktuellen Einstellungen Ihres Systems gespeichert. Bewahren Sie Ihre Backups außerdem an einem sicheren Ort auf, da sicherheitsrelevante Daten wie z. B. Zertifikate und kryptografische Schlüssel darin enthalten sind. Prüfen Sie die Backup-Datei nach der Generierung immer auf Lesbarkeit. Es ist außerdem ratsam, durch ein externes MD5-Programm eine Prüfsumme zu generieren, die es Ihnen auch später ermöglicht, die Integrität der Backup-Datei zu prüfen.

4.5.1 Backup/Wiederherstellen

Auf der Registerkarte *Verwaltung > Backup/Wiederherstellen > Backup/Wiederherstellen* können Sie Backups erstellen, importieren, wiederherstellen, herunterladen und senden sowie bestehende Backups löschen.

Verfügbare Backups

Dieser Abschnitt ist nur sichtbar, wenn bereits mindestens ein Backup erstellt wurde, entweder automatisch oder manuell (siehe Abschnitt *Backup erstellen*).

Alle Backups sind mit ihrem Erstellungsdatum und -zeitpunkt, ihrer UTM-Versionsnummer, ihrem Ersteller und Kommentar aufgelistet.

Sie können ein Backup herunterladen, wiederherstellen, löschen oder versenden.

- **Herunterladen:** Öffnet ein Dialogfenster, in dem Sie wählen können, ob Sie die Datei verschlüsselt (Kennwort eingeben) oder unverschlüsselt herunterladen wollen. Klicken Sie auf *Backup herunterladen*. Sie werden gebeten, einen Ort im Dateisystem auszuwählen, an dem die heruntergeladene Datei gespeichert werden soll.
    - **Vor dem Herunterladen verschlüsseln:** Bevor Sie ein Backup herunterladen oder versenden, haben Sie die Möglichkeit, es zu verschlüsseln. Die Verschlüsselung erfolgt durch Blowfish-Verschlüsselung im CBC-Modus. Geben Sie ein Kennwort ein (ein zweites Mal zur Bestätigung). Nach diesem Kennwort werden Sie gefragt, wenn Sie das Backup importieren wollen. Für verschlüsselte Backups lautet die Dateierweiterung `ebf`, für unverschlüsselte Backups `abf`).

      Hinweis – Ein Backup enthält Administrationskennwörter, das Hochverfügbarkeitskennwort (falls konfiguriert) sowie alle RSA-Schlüssel und X.509-Zertifikate. Da es sich dabei um vertrauliche Informationen handelt, ist es ratsam, Backups zu verschlüsseln.

- **Wiederherstellen:** Ersetzt die aktuellen Systemeinstellungen durch die in einem Backup gespeicherten Einstellungen. Hinterher müssen Sie sich neu anmelden. Im Fall, dass das Backup alle Daten enthält, können Sie sich direkt anmelden. Wenn das ausgewählte Backup nicht alle Daten enthält (siehe Abschnitt *Backup erstellen*), müssen Sie die erforderlichen Daten während des Anmeldevorgangs eingeben. Wenn lediglich die Hostdaten aus dem gewählten Backup entfernt wurden, können Sie bei Bedarf eine weitere Administrator-E-Mail-Adresse hinzufügen. Diese wird an Stellen eingesetzt, an denen bisher kein Empfänger eingetragen war, und als zusätzliche Adresse dort, wo mehrere Empfänger möglich sind.
    - Backups von USB-Flashspeicher wiederherstellen: Sie können unverschlüsselte Backup-Dateien (Dateierweiterung `abf`) von einem mit FAT formatierten USB-Flashspeicher wie z. B. einem USB-Stick wiederherstellen. Um ein Backup von

einem USB-Flashspeicher wiederherzustellen, kopieren Sie die Backup-Datei auf den USB-Flashspeicher und schließen Sie ihn an die Sophos UTM an, bevor Sie das System starten. Befinden sich mehrere Backup-Dateien auf dem Speichergerät, wird die lexikografisch erste Datei verwendet (Zahlen vor Buchstaben). Angenommen, die Backup-Dateien `gateway_backup_2012-04-17.abf` und `2011-03-20_gateway_backup.abf` befinden sich beide auf dem USB-Flashspeicher. Beim Starten wird die zweite Datei verwendet, weil sie mit einer Zahl beginnt, obwohl sie viel älter ist als die andere Datei.

Nach der erfolgreichen Wiederherstellung eines Backups wird eine Sperrdatei (engl. lock file) angelegt. Diese verhindert, dass ein- und dasselbe Backup immer wieder installiert wird, während der USB-Flashspeicher noch eingesteckt ist. Sollten Sie ein vorangegangenes Backup dennoch erneut installieren wollen, so müssen Sie den betreffenden Rechner zunächst ohne angeschlossenen USB-Flashspeicher neu starten. Dabei werden alle Sperrdateien gelöscht. Wenn Sie den Rechner nun erneut mit angeschlossenem USB-Flashspeicher hochfahren, kann dasselbe Backup installiert werden.

- **Löschen:** Löscht ein Backup aus der Liste. Mit dem Löschen-Symbol unterhalb der Liste können Sie alle ausgewählten Backups löschen. Um Backups auszuwählen, klicken Sie auf die Auswahlkästchen links von den Backups oder verwenden Sie die Auswahlliste unten, um alle Backups auszuwählen.
- **Senden:** In einem Dialogfenster können Sie die E-Mail-Empfänger festlegen. Standardmäßig sind die auf der Registerkarte *Automatische Backups* angegebenen Adressen ausgewählt. Entscheiden Sie dann, ob Sie die Datei verschlüsselt (Kennwort angeben) oder unverschlüsselt senden möchten. Klicken Sie auf *Jetzt senden*, um das Backup zu senden.
    - **Vor dem Senden verschlüsseln:** Siehe oben: *Vor dem Herunterladen verschlüsseln*

Backup erstellen

Backups sind nicht nur nützlich, wenn Sie Ihr System nach einer (nicht beabsichtigten) Änderung oder einem Ausfall wiederherstellen möchten. Sie können auch als Vorlagen genutzt werden, um Systeme mit einer ähnlichen Konfiguration einzurichten. Diese Systeme sind dann quasi vorkonfiguriert, was eine enorme Zeitersparnis darstellen kann. Zu diesem Zweck können Sie vor der Erstellung bestimmte Daten von einem Backup entfernen, z. B. Hostname, Zertifikate usw.

Um ein Backup mit den aktuellen Systemeinstellungen zu erzeugen, gehen Sie folgendermaßen vor:

1. **Geben Sie im Abschnitt *Backup erstellen* einen Kommentar** ein (optional).
   Der Kommentar wird neben dem Backup in der Backup-Liste angezeigt.
2. **Nehmen Sie die folgenden Einstellungen vor** (optional):

   Eindeutige Standortdaten entfernen: Wählen Sie diese Option, um das Backup ohne Host-spezifische Daten zu erstellen. Dies umfasst Hostnamen, System-ID, SNMP-Daten, HA-Daten, Lizenz, Shell-Benutzerkennwörter, Anonymisierungskennwörter, alle Zertifikate, öffentliche und private Schlüssel, Fingerabdrücke und Schlüssel von Email Protection, Web Protection, Client-Authentifizierung, IPsec, SSL-VPN, RED, WebAdmin, Web Application Firewall und Proxys.
   Solche Backups ermöglichen es Ihnen, mehrere ähnliche Systeme bequem anzulegen. Sie sollten allerdings einige Punkte beachten: 1) Nach der Wiederherstellung wird die Grundkonfiguration-Seite (Basic System Setup) angezeigt. 2) Nur die erste Schnittstelle ist konfiguriert, wobei die primäre IP-Adresse während der Installation konfiguriert wurde. Alle anderen Schnittstellen werden deaktiviert und erhalten die IP-Adresse 0.0.0.0.

   Achtung – Obwohl die meisten Host-spezifischen Daten entfernt werden, enthält eine solche Backup-Vorlage dennoch vertrauliche Daten wie Benutzerkennwörter. Deshalb ist es ratsam, Backup-Vorlagen zu verschlüsseln.

   Administrative E-Mail-Adressen entfernen: Wählen Sie diese Option, um die Administrator-E-Mail-Adressen, die in verschiedenen Bereichen der UTM verwendet werden, z.B. Postmaster-Adressen in Email Protection, Benachrichtigungen usw., zu entfernen.Diese Option ist besonders für IT-Partner sinnvoll, die Sophos UTM-Appliances an Kundenstandorten einrichten.
3. **Klicken Sie auf *Backup jetzt erzeugen*.**
   Das Backup wird in der Liste der verfügbaren Backups angezeigt.

   Falls ein Backup mit einer oder beiden der gewählten Optionen erzeugt wurde, enthält der Backup-Eintrag einen entsprechenden zusätzlichen Hinweis.

Backup importieren

Um ein Backup zu importieren, klicken Sie auf das Ordnersymbol und wählen Sie eine Backup-Datei, die hochgeladen werden soll. Klicken Sie danach auf *Hochladen starten*. Wenn Sie ein verschlüsseltes Backup importieren möchten, müssen Sie zunächst das Kennwort eingeben.

Beachten Sie, dass beim Import des Backups noch keine Wiederherstellung durchgeführt wird.Das Backup wird lediglich zur Liste *Verfügbare Backups* hinzugefügt.

4.5.2 Automatische Backups

Auf der Registerkarte *Verwaltung > Backup/Wiederherstellen > Automatische Backups* haben Sie die Möglichkeit, verschiedene Optionen zur automatischen Erstellung von Backups zu konfigurieren. Um Backups automatisch erzeugen zu lassen, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Automatische Backups* automatische Backups.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und die Abschnitte *Optionen* sowie *Backups per E-Mail versenden* können nun bearbeitet werden.

2. **Legen Sie das Zeitintervall fest.**
   Automatisch erzeugte Backups können in verschiedenen Zeitintervallen erzeugt werden.

   Sie haben die Auswahl zwischen täglich, wöchentlich und monatlich.

3. **Legen Sie die maximale Anzahl der zu speichernden Backups fest.**
   Backups können bis zu der hier angegebenen Anzahl gespeichert werden. Nachdem die maximale Anzahl erreicht worden ist, werden die ältesten Backup-Dateien gelöscht.

   Beachten Sie, dass dies nur auf automatisch erzeugte Backup-Dateien zutrifft. Manuell erzeugte Backup-Dateien und vor einer Systemaktualisierung automatisch erzeugte Backup-Dateien werden nicht gelöscht.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um Backup-Dateien Ihrer UTM nicht mühevoll manuell speichern zu müssen, können Sie Backup-Dateien an eine Liste von E-Mail-Adressen schicken lassen.

Empfänger: Automatisch erzeugte Backup-Dateien werden an diejenigen Benutzer gesendet, die im Feld *Empfänger* eingetragen sind. Es können mehrere Adressen angegeben werden. Standardmäßig ist die E-Mail-Adresse des Administrators voreingestellt.

E-Mail-Backups verschlüsseln: Darüber hinaus haben Sie die Möglichkeit, das Backup zu verschlüsseln (3DES-Verschlüsselung).

Kennwort: Wenn Sie die Option *E-Mail-Backups verschlüsseln* gewählt haben, geben Sie ein Kennwort ein (ein zweites Mal zur Bestätigung). Nach diesem Kennwort werden Sie gefragt, wenn Sie das Backup importieren wollen.

Automatisch erzeugte Backups werden in der Liste *Verfügbare Backups* auf der Registerkarte *Backup/Wiederherstellen* angezeigt und sind mit dem Hinweis `System` in der Spalte *Ersteller* versehen. Von dort aus können sie genau wie manuell erzeugte Backup-Dateien wiederhergestellt, heruntergeladen oder gelöscht werden.

4.6 Benutzerportal

Das Benutzerportal von Sophos UTM ist eine besondere Browser-basierte Anwendung, die autorisierten Benutzern personalisierte E-Mail-Dienste und Dienste für den Fernzugriff zur Verfügung stellt.Der Zugriff ist über die URL der Sophos UTM möglich, zum Beispiel `https://192.168.2.100`. (Beachten Sie das HTTPS-Protokoll und die fehlende Portnummer `4444`, die Sie normalerweise eingeben würden, um auf die WebAdmin-Schnittstelle zugreifen zu können.)

Das Benutzerportal umfasst unter anderem die E-Mail-Quarantäne, die jene Nachrichten enthält, die entweder mit schädlicher Software infiziert sind, verdächtige Anhänge besitzen, als Spam identifiziert wurden oder Ausdrücke enthalten, die explizit untersagt sind.

Benutzer können auf der Anmeldeseite eine Sprache aus der Auswahlliste auswählen, die sich rechts in der Kopfleiste befindet.

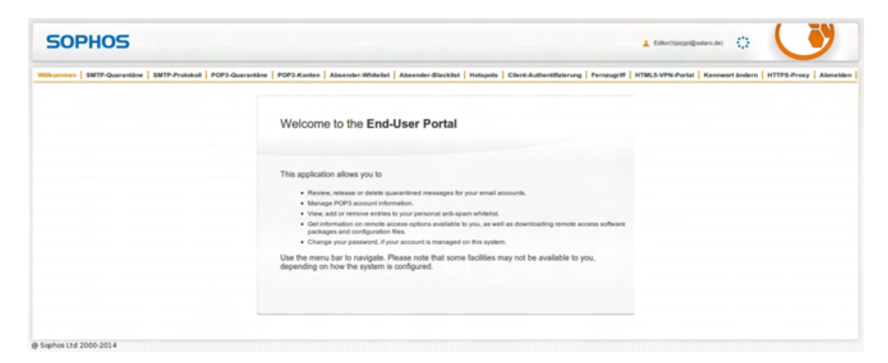


Bild 11 Benutzerportal: Begrüßungsseite

Über das Benutzerportal haben Benutzer Zugriff auf die folgenden Dienste:

- **SMTP-Quarantäne:** Benutzer können sich Nachrichten in Quarantäne anschauen und gegebenenfalls freigeben. Welche Arten von Nachrichten sie freigeben dürfen, kann auf der Registerkarte *Email Protection* > *Quarantänebericht* > *Erweitert* festgelegt werden. (Die Registerkarte heißt *Mail-Quarantäne*, wenn POP3 deaktiviert ist.)
- **SMTP Log:** Benutzer haben hier Einblick in das SMTP-Protokoll ihres Mailverkehrs.(Die Registerkarte heißt *Mail-Protokoll*, wenn POP3 deaktiviert ist.)
- **POP3-Quarantäne:** Benutzer können sich Nachrichten in Quarantäne anschauen und gegebenenfalls freigeben. Welche Arten von Nachrichten sie freigeben dürfen, kann auf der Registerkarte *Email Protection* > *Quarantänebericht* > *Erweitert* festgelegt werden. (Die Registerkarte heißt *Mail-Quarantäne*, wenn SMTP deaktiviert ist.)
- **POP3-Konten:** Benutzer können hier ihre Zugangsdaten für POP3-Konten eingeben, die sie verwenden. Es werden nur Spam-E-Mails, für die POP3-Kontozugangsdaten hinterlegt sind, im Benutzerportal angezeigt. Benutzer, für die POP3-Kontozugangsdaten gespeichert sind, erhalten einen eigenständigen Quarantänebericht für jede E-Mail-Adresse. Beachten Sie, dass zugelassene POP3-Server auf der Registerkarte *Email Protection* > *POP3* > *Erweitert* eingetragen sein müssen.
- **Absender-Whitelist:** Benutzer können eine Positivliste für bestimmte Absender anlegen. Dadurch werden Nachrichten von diesen Absendern nicht als Spam angesehen. E-Mails mit Viren oder unscannbare E-Mails werden jedoch stets unter Quarantäne gestellt. In die Whitelist können sowohl einzelne gültige E-Mail-Adressen (z. B. `mmustermann@beispiel.de`) als auch Adressen einer spezifischen Domäne eingetragen werden, wobei ein Asterisk als Platzhalter dient (z. B. `*@beispiel.de`).
- **Absender-Blacklist:** Hier können Benutzer E-Mail-Absender auf die Blacklist setzen, z. B. `phishing@hotmail.com`, oder auch ganze Domänen, z. B. `*@hotmail.com`. Die Blacklist wird sowohl auf SMTP- als auch auf POP3-E-Mails angewendet, wenn diese auf dem System aktiviert sind. Absender können auf die Blacklist gesetzt werden, indem man auf das Plussymbol klickt, die Adresse eingibt und zum Speichern auf das Häkchen klickt. SPX
- **Hotspots:** Hier finden Benutzer die Zugriffsdaten von Hotspots und können diese verwalten. Diese Registerkarte ist nur dann vorhanden, wenn für einen bestimmten Benutzer mindestens ein Hotspot aktiviert wurde. Für Hotspots mit täglicher Kennwortänderung wird das aktuelle Kennwort angezeigt, das auch geändert werden kann. Für Hotspots, die über Voucher genutzt werden können, können Voucher erstellt, ausgedruckt, exportiert und gelöscht werden. Auf einer Liste der erstellten Voucher werden Nutzungsinformationen angezeigt.Weitere Informationen finden Sie unter *Wireless Protection* > *Hotspots*.

- **Client-Authentifizierung:** Hier können die Benutzer eine Einrichtungsdatei von Sophos Authentication Agent (SAA) herunterladen. Der SAA kann als Authentifizierungsmethode für den Webfilter genutzt werden. Die Registerkarte *Client-Authentifizierung* ist nur dann verfügbar, wenn die entsprechende Funktion aktiviert wurde.Weitere Informationen finden Sie unter *Definitionen & Benutzer* > *Client-Authentifizierung*.
- **OTP-Token:** Hier finden die Benutzer einen oder mehrere QR-Codes sowie die entsprechenden Detailinformationen für die Konfiguration des Dienstes der UTM für einmalige Kennwörter (OTP) auf ihren Mobilgeräten.Weitere Informationen finden Sie unter *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Einmaliges Kennwort (OTP)*.
- **Fernzugriff:** Benutzer können hier Client-Software für den Fernzugriff sowie für sie bereitgestellte Konfigurationsdateien herunterladen. Der Menüpunkt *Fernzugriff* ist allerdings nur zu sehen, wenn für den jeweiligen Benutzer der Fernzugriff aktiviert wurde.
- **HTML5-VPN-Portal:** Hier können Benutzer über vordefinierte Dienste VPN-Verbindungen zu vordefinierten Hosts öffnen. Diese Registerkarte ist nur dann vorhanden, wenn für den jeweiligen Benutzer mindestens eine VPN-Verbindung aktiviert wurde. Weitere Informationen finden Sie unter *Fernzugriff* > *HTML5-VPN-Portal*.
- **Kennwort ändern:** Benutzer können hier ihr Kennwort für den Zugang zum Benutzerportal ändern.
- **HTTPS-Proxy:** Benutzer können von hier das HTTP/S-Proxy-CA-Zertifikat importieren, damit keine Fehlermeldungen mehr angezeigt werden, wenn sie sichere Websites besuchen. Nach dem Klicken auf die Schaltfläche *Proxy-CA-Zertifikat importieren* wird der Benutzer von seinem Browser gefragt, ob er der CA für verschiedene Zwecke vertraut. Weitere Informationen erhalten Sie unter *Web Protection* > *Filteroptionen* > *HTTPS-CAs*.
- **Abmelden:** Klicken Sie hier, um sich vom Benutzerportal abzumelden. Das ist allerdings nur nötig, wenn Sie beim Anmelden *An meine Anmeldung erinnern* markiert hatten – dabei wird ein Cookie angelegt – und Sie sich nun explizit abmelden möchten. Dabei wird der Cookie gelöscht.Ansonsten gibt es keinen Grund, die *Abmelden*-Funktion zu verwenden; es reicht aus, die Registerkarte des Browsers oder das Browserfenster zu schließen.

4.6.1 Allgemein

Auf der Registerkarte *Verwaltung* > *Benutzerportal* > *Allgemein* können Sie das Benutzerportal aktivieren. Zudem können Sie festlegen, welchen Netzwerken und welchen Benutzern Zugriff auf das Benutzerportal gewährt werden soll.

Um den Zugang zum Benutzerportal zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie das Benutzerportal.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Benutzerportal-Optionen* kann nun bearbeitet werden.

2. **Wählen Sie die zugelassenen Netzwerke aus.**
   Wählen Sie die Netzwerke aus, die Zugriff auf das Benutzerportal haben sollen, oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

3. **Wählen Sie die zugelassenen Benutzer aus.**
   Wählen Sie die Benutzer oder Benutzergruppen aus, die Zugriff auf das Benutzerportal haben sollen, oder fügen Sie neue Benutzer hinzu. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer* erläutert.

   Wenn Sie nicht allen Benutzern Zugriff gestatten möchten, deaktivieren Sie die Option *Alle Benutzer zulassen* und wählen Sie die Benutzer oder Benutzergruppen einzeln aus.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

4.6.2 Erweitert

Auf der Registerkarte *Erweitert* können Sie einen alternativen Hostnamen und eine Portnummer für das Benutzerportal definieren sowie Sprach- und Sicherheitseinstellungen vornehmen.

Sprache

Während der Anmeldung wertet das Benutzerportal die Spracheinstellungen des Webbrowsers aus und lädt das entsprechende Gebietsschema, um das Benutzerportal in der Standardsprache des Browsers anzuzeigen. Sollte der Browser eine Sprache als Standardeinstellung haben, die im Benutzerportal nicht verfügbar ist, können Sie hier angeben,

welche Sprache ersatzweise verwendet werden soll. Benutzer haben darüber hinaus die Möglichkeit, eine Sprache auf der Anmeldeseite des Benutzerportals zu wählen.

Sicherheit

Das Benutzerportal verwendet Cookies zur Sitzungsverwaltung. Dauerhafte Cookies ermöglichen dem Benutzer, nach dem Schließen einer Sitzung später zurückzukehren, ohne sich neu anmelden zu müssen. Cookies können jederzeit vom Benutzer gelöscht werden, indem er im Benutzerportal auf *Abmelden* klickt.

Portal-Einträge deaktivieren

Für die hier angegebenen Funktionen wird im Benutzerportal ein Menüeintrag angezeigt, falls die entsprechende Funktion im WebAdmin aktiviert wurde. Sie können aber Menüeinträge bestimmen, die *nicht* im Benutzerportal angezeigt werden sollen. Wählen Sie hierzu die entsprechende(n) Option(en) aus und klicken Sie auf *Übernehmen*.

Netzwerkeinstellungen

Hostname: Standardmäßig ist der Hostname der UTM voreingestellt, wie er auf der Registerkarte *Verwaltung* > *Systemeinstellungen* > *Hostname* angegeben ist. Wenn Sie allerdings Zugriff auf das Benutzerportal über das Internet gestatten möchten, dann ist es sinnvoll, hier einen alternativen Hostnamen einzutragen, der öffentlich aufgelöst werden kann.

Lausch-Adresse: Der Standardwert lautet *Any*. Wenn Sie die Web Application Firewall verwenden, müssen Sie eine feste Schnittstellenadresse angeben, auf der der Dienst auf Verbindungen zum Benutzerportal lauscht. Diese Einstellung ist notwendig, damit die Verbindungsverwaltung für das Benutzerportal und die Web Application Firewall die eingehenden SSL-Verbindungen unterscheiden können.

Port: Standardmäßig ist der Port `443` für HTTPS voreingestellt. Sie können den Port jedoch auf einen beliebigen Wert zwischen `1024` und `65535` ändern. Beachten Sie, dass Sie weder den Port `10443` noch den *WebAdmin-TCP-Port* auswählen können, der auf der Registerkarte *Verwaltung* > *WebAdmin-Einstellungen* > *Erweitert* konfiguriert ist. Unabhängig vom gewählten Port kann das Benutzerportal stets nur über HTTPS aufgerufen werden.

Begrüßungstext

Sie können den Begrüßungstext des Benutzerportals anpassen. Einfache HTML-Befehle und Hyperlinks sind gestattet.

Hinweis – Der Begrüßungstext kann nicht geändert werden, wenn Sie eine Home-Use-Lizenz verwenden.

4.7 Benachrichtigungen

Sophos UTMverfügt über eine Benachrichtigungsfunktion, die Sie sofort per E-Mail oder SNMP über alle sicherheitsrelevanten Vorgänge auf der UTM informiert – entweder per E-Mail oder SNMP-Trap. Alle Ereignisse, die für einen Administrator von Interesse sein könnten, haben ihre eigenen Fehler-, Warn- und Informations-Codes. Welche Benachrichtigungen verschickt werden, hängt von den Einstellungen ab, die Sie auf der Registerkarte *Benachrichtigungen* vorgenommen haben.

4.7.1 Allgemein

Auf der Registerkarte *Verwaltung > Benachrichtigungen > Allgemein* können Sie die Absenderadresse (d. h. die *From*-Adresse) konfigurieren, die für das Versenden von Benachrichtigungen von der UTM verwendet werden soll. Standardmäßig ist dies `do-not-reply@fw-notify.net`. Falls Sie diese Einstellung ändern möchten, ist es ratsam, eine E-Mail-Adresse aus Ihrer Domäne zu wählen, da manche Mail-Server überprüfen, ob die Absender-Adresse einer empfangenen Nachricht tatsächlich existiert.

Darüber hinaus können Sie einen oder mehrere Empfänger für die Benachrichtigungen der UTM festlegen. Standardmäßig ist dies die E-Mail-Adresse des Administrators, die Sie während der ersten Einrichtung angegeben haben.

Benachrichtigungen begrenzen: Einige sicherheitsrelevante Ereignisse, z. B. erkannte Angriffsversuche, erzeugen eine Vielzahl von Benachrichtigungen, was schnell dazu führen kann, dass die Postfächer der Empfänger förmlich überlaufen. Zu diesem Zweck verfügt die Sophos UTM über angemessene Voreinstellungen, welche die Anzahl der Benachrichtigungen, die pro Stunde verschickt werden, begrenzen. Falls Sie diese Option deaktivieren, erzeugt jedes sicherheitsrelevante Ereignis eine Benachrichtigung; vorausgesetzt natürlich, dieses Ereignis ist auf der Registerkarte *Verwaltung > Benachrichtigungen > Benachrichtigungen* entsprechend konfiguriert.

Gerätespezifischer Text

Hier können Sie eine Beschreibung der Sophos UTM eingeben, z. B. den Standort. Diese wird dann in den Benachrichtigungen angezeigt, die verschickt werden.

4.7.2 Benachrichtigungen

Benachrichtigungen sind in drei Kategorien unterteilt:

- **CRIT:** Benachrichtigungen über kritische Ereignisse, die den fehlerfreien Betrieb der UTM gefährden.
- **WARN:** Warnhinweise über potenzielle Probleme, die Ihre Aufmerksamkeit erfordern, z. B. das Überschreiten von Schwellenwerten.
- **INFO:** Rein informative Benachrichtigungen, z. B. bezüglich des Neustarts einer Systemkomponente.

Für jedes einzelne Ereignis können Sie bestimmen, ob eine Benachrichtigung als E-Mail oder SNMP-Trap verschickt werden soll.

4.7.3 Erweitert

Für den Fall, dass Ihre UTM E-Mails nicht direkt senden kann, können Sie einen Smarthost für den E-Mail-Versand einrichten. Gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den *Externen SMTP*-Server auf der Registerkarte *Verwaltung > Benachrichtigungen > Erweitert*.**
   Klicken Sie auf den Schieberegler.
2. **Geben Sie Ihren Smarthost ein**.
   Sie können dafür Drag-and-Drop verwenden. Der Port ist auf den SMTP-Port `25` voreingestellt.
   - **TLS verwenden:** Wählen Sie diese Option, wenn Sie TLS für den Versand von Benachrichtigungen erzwingen wollen. Beachten Sie, dass Benachrichtigungen nicht versendet werden, wenn der Smarthost TLS nicht unterstützt.
3. **Legen Sie die Authentifizierungseinstellungen fest.**
   Falls der Smarthost Authentifizierung erfordert, wählen Sie das Auswahlkästchen *Authentifizierung* und geben Sie den entsprechenden Benutzernamen und das Kennwort ein.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

4.8 Anpassungen

Auf den Registerkarten des Menüs *Verwaltung* > *Anpassungen* können Sie die Vorlagen für Statusmeldungen und E-Mail-Benachrichtigungen, die von Sophos UTM erstellt werden, anpassen und lokalisieren. Damit ist es möglich, diese Meldungen an die Richtlinien und die Corporate Identity Ihres Unternehmens anzupassen.

Zusätzlich können Sie benutzerdefinierte Web-Vorlagen hochladen und bearbeiten, um Meldungen über blockierte Seiten oder andere Benachrichtigungen noch stärker zu verändern.

Hinweis – Anpassungen sind nicht möglich, wenn Sie eine Home-Use-Lizenz verwenden.

4.8.1 Allgemein

Auf der Registerkarte *Verwaltung* > *Anpassung* > *Allgemein* können Sie allgemeine Einstellungen für Statusmeldungen vornehmen, die Benutzern angezeigt werden. Beachten Sie, dass UTF-8/Unicode unterstützt wird.

Das Beispiel unten zeigt die anpassbaren globalen Optionen (*Firmenlogo* und *Firmenspezifischer Text*) in einer beispielhaften „Inhalt blockiert“-Nachricht, die auf der Seite *Verwaltung* > *Anpassungen* > *Web-Meldungen* angepasst werden kann.

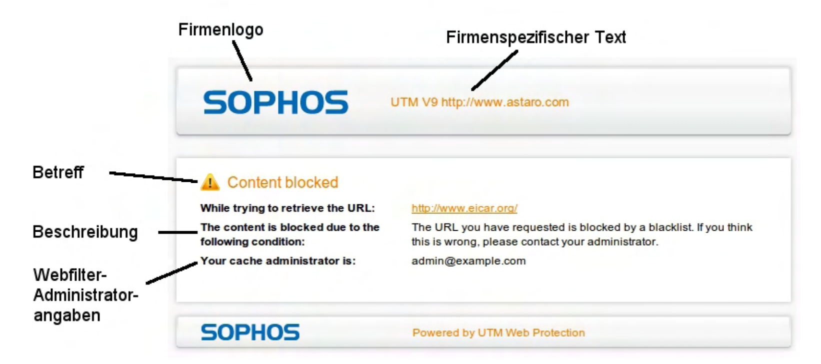


Bild 12 Anpassung: Beispiel einer blockierten Webseite mit Angabe der anpassbaren Elemente

Firmenlogo

Hier können Sie Ihr eigenes Firmenlogo/-banner (nur im `png`-Format) hochladen, das in den folgenden Fällen verwendet wird:

- Web-Meldungen
- Blockierte POP3-E-Mails
- Statusmeldungen zur Aufhebung der Quarantäne (werden angezeigt, wenn eine als Spam eingestufte E-Mail über den Quarantänebericht aus der Quarantäne freigegeben oder auf die Positivliste (Whitelist) gesetzt wurde)
- Quarantänebericht

Einige der Benutzermeldungen sind für das Standard-Logo optimiert (195 x 73 Pixel mit transparentem Hintergrund). Um ein optimales Ergebnis zu erhalten, sollten Sie ein Bild mit den gleichen Eigenschaften verwenden.

Um ein Logo hochzuladen:

1. **Öffnen Sie das Dialogfenster *Datei hochladen*.**
   Klicken Sie dazu auf das Ordnersymbol neben dem Feld *Neues Logo hochladen*.

   Das Dialogfeld *Datei hochladen* öffnet sich.

2. **Wählen Sie das Logo aus.**
   Wechseln Sie in das Verzeichnis, in dem sich das Firmenlogo befindet.

   Wählen Sie das Logo aus und klicken Sie auf *Hochladen starten*.

3. **Klicken Sie auf *Übernehmen*.**
   Das Logo wird hochgeladen und ersetzt dabei die zuvor installierte Datei.

Firmenspezifischer Text

Hierbei handelt es sich um den Text unterhalb des Firmenlogos auf der Standard-Fehlermeldungsseite, die vom Browser angezeigt wird, wenn ein Benutzer eine Website öffnet, die vom Virenscanner oder dem Inhaltsfilter von Sophos UTM blockiert wird. Sie können hier z. B. die Kontaktdaten des Administrators eintragen.

4.8.2 Web-Meldungen

Sie können die Texte von Webfilter-Meldungen anpassen, die von der Sophos UTM angezeigt werden. Meldungen werden beispielsweise angezeigt, wenn Benutzer bestimmte Dateien nicht herunterladen dürfen, weil sie zu groß sind, von einem bestimmten Typ sind oder einen Virus enthalten. Meldungen werden auch angezeigt, wenn Benutzer versuchen, auf gesperrte Webseiten oder Anwendungen zuzugreifen, wenn sie Dateien herunterladen oder wenn sie sich mit der UTM authentifizieren müssen. Sie können Meldungen in andere Sprachen übersetzen oder sie zusätzlich um Support-Kontaktinformationen erweitern, um nur einige Beispiele zu nennen.

Hinweis – Der Text, den Sie hier auf der Registerkarte *Web-Meldungen* eingeben, kann in benutzerspezifischen Web-Vorlagen verwendet werden.Weitere Informationen finden Sie unter *Web-Vorlagen*.

Die folgenden Vorlagen können angepasst werden:

Inhalt blockieren

- **Surf Protection:** Diese Meldung wird angezeigt, wenn ein Benutzer auf eine Webseite zugreifen möchte, deren URL mit einer Kategorie übereinstimmt, die blockiert werden soll, oder wenn der Ruf der Seite unter dem eingestellten Schwellenwert liegt. Mehr Informationen finden Sie unter *Web Protection* > *Webfilter*.
- **Blacklist:** Diese Meldung wird angezeigt, wenn ein Benutzer auf eine Webseite zugreifen möchte, deren URL blockiert werden soll. Um URLs zur Negativliste hinzuzufügen, gehen Sie auf die Seite *Web Protection* > *Webfilter* > *Richtlinien* > *Websitefilter*.

- **MIME-Typ:** Diese Meldung wird angezeigt, wenn ein Benutzer eine Datei mit einem MIME-Typ anfordert, der blockiert werden soll. Weitere Informationen zum Festlegen von MIME-Typen finden Sie unter *Web Protection* > *Webfilter* > *Richtlinien* > *Downloads*.
- **Dateierweiterung:** Diese Meldung wird angezeigt, wenn ein Benutzer eine Datei mit einer Erweiterung anfordert, die blockiert werden soll. Weitere Informationen zum Festlegen von Dateierweiterungen finden Sie unter *Web Protection* > *Webfilter* > *Richtlinien* > *Downloads*.
- **Dateigröße:** Diese Meldung wird angezeigt, wenn ein Benutzer eine Datei anfordert, die die maximal erlaubte Dateigröße überschreitet. Die maximale Download-Dateigröße legen Sie hier fest: *Web Protection* > *Webfilter* > *Richtlinien* > *Downloads*.
- **Application Control:** Diese Meldung wird angezeigt, wenn ein Benutzer versucht, einen Netzwerkverkehrstyp zu verwenden, der durch Application Control blockiert wird.Weitere Informationen zu Application Control finden Sie im Kapitel *Web Protection* > *Application Control*.
- **Virus gefunden:** Diese Meldung wird angezeigt, wenn eine Datei blockiert wird, die einen Virus enthält. Weitere Informationen über Virenschutzeinstellungen finden Sie unter *Web Protection* > *Webfilter* > *Richtlinien* > *Antivirus*.

Download/Scan

- **Download läuft:** Diese Meldung wird angezeigt, während eine Datei heruntergeladen wird. Siehe *Download-Verwaltung*.
- **Virenscan läuft:** Diese Meldung wird angezeigt, während die UTM Dateien auf schädlichen Inhalt prüft. Siehe *Download-Verwaltung*.
- **Download abgeschlossen:** Diese Meldung wird angezeigt, nachdem eine Datei komplett heruntergeladen, gescannt und für sicher befunden wurde.Siehe *Download-Verwaltung*.

Authentifizierung

- **Transparenzmodus mit Authentifizierung:** Diese Option gilt nur für den Fall, dass Sie den Webfilter im Transparenzmodus betreiben und die Authentifizierungsmethode „Browser“ gewählt haben. Weitere Informationen finden Sie unter *Web Protection* > *Webfilter-Profile* > *Proxy-Profile*. Der Text wird auf der Authentifizierungsseite angezeigt, auf der sich Benutzer einloggen müssen, bevor sie den Webfilter benutzen dürfen. Wenn das Feld *Nutzungsbedingungen* Text enthält, wird dieser auf der Authentifizierungsseite angezeigt. Wenn das Feld leer ist (Standard), werden keine Nutzungsbedingungen angezeigt.

- **Inhaltsblockierung umgehen:** Diese Meldung wird angezeigt, wenn eine Seite durch Surf Protection blockiert ist und die Option, die Blockierung zu umgehen, aktiv ist (siehe *Web Protection* > *Filteroptionen* > *Benutzer umgehen*). Wenn das Feld *Nutzungsbedingungen* Text enthält, wird dieser auf der Authentifizierungsseite angezeigt. Wenn das Feld leer ist (Standard), werden keine Nutzungsbedingungen angezeigt.

Fehler

- **Serverfehler:** Diese Meldung wird angezeigt, wenn bei der Bearbeitung einer Benutzeranfrage ein Fehler auftritt.

Administratorinformationen: Hier können Sie Informationen zum Administrator angeben, der den Webfilter verwaltet, einschließlich seiner E-Mail-Adresse.

4.8.2.1 Web-Meldung ändern

Um eine Meldung des Typs Blockierter Inhalt, Download/Scan, Authentifizierung oder Fehler zu ändern:

1. **Wählen Sie die Meldung aus.**
   Wählen Sie in der Auswahlliste *Seite* die Benutzermeldung aus, die Sie bearbeiten möchten.

   Betreff und *Beschreibung* dieser Meldung werden angezeigt.

2. **Ändern Sie den Betreff und/oder die Beschreibung.**
   Bearbeiten Sie den Standardtext nach Bedarf.

3. **Klicken Sie auf *Übernehmen*.**
   Die Textänderungen werden gespeichert.

4.8.2.2 Download-Verwaltung

Wenn der Webfilter aktiviert ist, zeigt der Webbrowser die folgenden Download-Seiten an, sobald ein Benutzer versucht, Inhalte von mehr als 1 MB Größe herunterzuladen, die keinen Text bzw. keine Bilder umfassen. Die Download-Seiten werden nicht angezeigt, wenn Video- oder Audio-Streams angefordert werden oder wenn mehr als 50 % einer Datei innerhalb von fünf Sekunden heruntergeladen wurden.

Die Informationen auf den Download-Seiten können auf der Registerkarte *Web-Meldungen* angepasst werden.

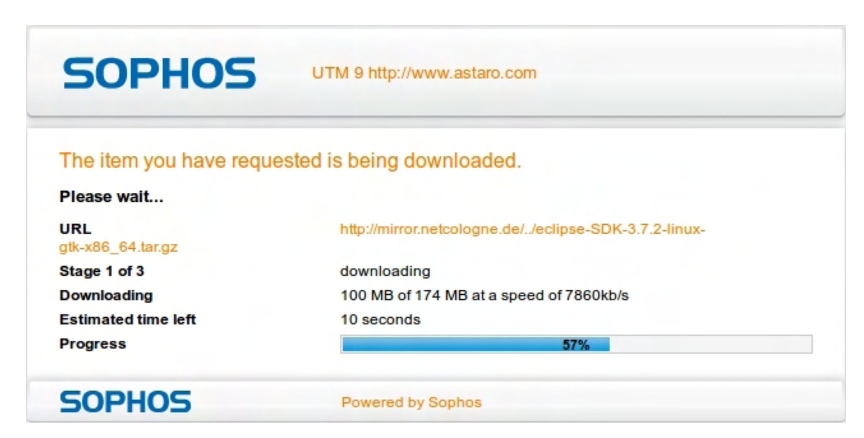


Bild 13 Anpassung: HTTP-Download-Seite Schritt 1 von 3 Datei wird heruntergeladen

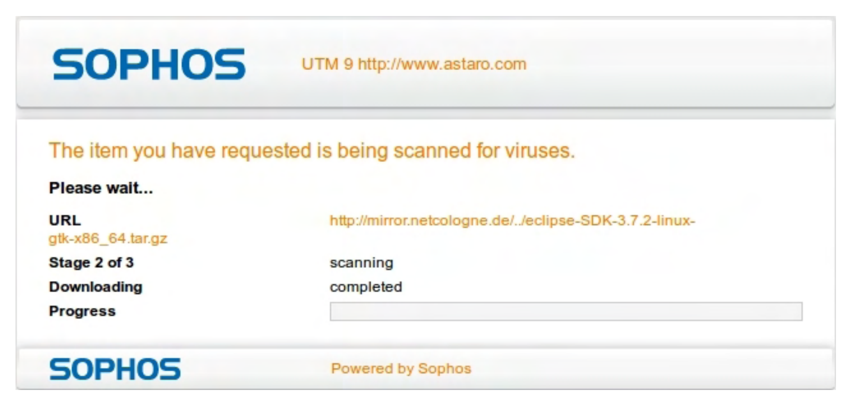


Bild 14 Anpassung: HTTP-Download-Seite Schritt 2 von 3 Virenscan

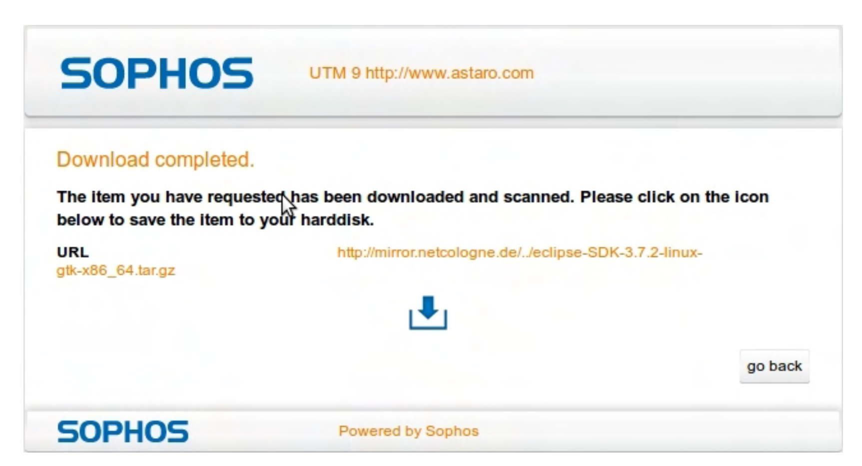


Bild 15 Anpassung: HTTP-Download-Seite Schritt 3 von 3 Herunterladen der Datei abgeschlossen

4.8.3 Web-Vorlagen

Um das Aussehen und den Inhalt von Meldungen, die Benutzern angezeigt werden, anzupassen, können Sie HTML-Dateien in Sophos UTM hochladen. Als Leitfaden bietet Sophos mehrere Beispiel-Vorlagen. Diese Vorlagen zeigen Ihnen, wie Sie Variablen verwenden können, um dynamisch Informationen einzufügen, die für die einzelnen Benutzermeldungen wichtig sind. Wenn beispielsweise eine Datei blockiert wird, weil sie einen Virus enthält, können Sie eine Variable verwenden, die den Namen des blockierten Virus einfügt.

4.8.3.1 Web-Vorlagen anpassen

Warnung – Das Anpassen von Sophos UTM-Benachrichtigungen ist ein Thema für Fortgeschrittene. Sie sollten diese Aufgabe nur dann angehen, wenn Sie ausreichende HTML- und JavaScript-Kenntnisse besitzen.

Sie können angepasste Versionen von Sophos UTM-Benachrichtigungen hochladen, einschließlich Meldungen über blockierten Inhalt, Statusmeldungen, Fehlermeldungen und Eingabeaufforderungen zur Authentifizierung. Die vier Beispielvorlagen enthalten Anwendungsbeispiele für Variablen und mehrere Bilder. Verwenden Sie für Ihre spezifischen Meldungen und Benachrichtigungen entweder die Beispielvorlagen als Basis oder laden Sie

Ihre eigenen HTML-Dateien hoch. Die gültigen Variablen sind im Artikel Using Variables in UTM Web Templates in der SophosKnowledgebase beschrieben.

Um Text aus einer Meldung zu verwenden, die auf der Registerkarte *Web-Meldungen* definiert ist, können Sie die entsprechende Variable in Ihre benutzerspezifische Vorlage einfügen.Weitere Informationen finden Sie unter *Web-Meldungen*.

Um die Beispielvorlagen und Bilder herunterzuladen, klicken Sie auf den folgenden Link und speichern Sie die .zip-Datei:

http://www.astaro.com/lists/Web_Templates.zip

4.8.3.2 Benutzerspezifische Web-Vorlagen und Bilder hochladen

Nachdem Sie Ihre benutzerspezifische Vorlage bearbeitet und gespeichert haben, können Sie sie in UTM hochladen.

Um eine Web-Vorlage oder ein Bild hochzuladen:

1. **Öffnen Sie das Dialogfenster *Datei hochladen*.**
   Klicken Sie auf das Ordner-Symbol neben dem Namen des Vorlagentyps, den Sie hochladen möchten, oder klicken Sie auf das Ordner-Symbol neben *Bilder*, wenn Sie ein Bild hochladen möchten.

   Hinweis – Die folgenden Dateitypen werden unterstützt: `.png`,`.jpg`, `.jpeg` und `.gif`.

   Das Dialogfeld *Datei hochladen* öffnet sich.

2. **Wählen Sie die Vorlage oder das Bild.**
   Wechseln Sie in das Verzeichnis, in dem sich die Vorlage oder das Bild befindet.

   Nachdem Sie die Vorlage oder das Bild ausgewählt haben, klicken Sie auf *Hochladen starten*.

   Das Dialogfenster *Datei hochladen* schließt sich.

3. **Klicken Sie auf *Übernehmen*.**
   Die Vorlage oder das Bild wird hochgeladen.

4.8.4 E-Mail-Mitteilungen

Passen Sie den Text in Benutzer-Mitteilungen an, die von den SMTP/POP3-Proxies von Sophos UTM generiert werden. Sie können die Vorlagen in andere Sprachen übersetzen oder sie zusätzlich um Kontaktinformationen erweitern, um nur einige Beispiele zu nennen. Die folgenden Meldungen können angepasst werden:

Quarantäne

Aus Quarantäne freigegebene E-Mail: Diese Meldung wird angezeigt, wenn eine E-Mail erfolgreich aus der Quarantäne freigegeben wurde.

Bei der Quarantäne-Freigabe der E-Mail ist ein Fehler aufgetreten: Diese Meldung wird angezeigt, wenn während der Freigabe einer E-Mail aus der Quarantäne ein Fehler aufgetreten ist.

POP3

POP3-Nachricht blockiert: Diese Meldung wird an den Empfänger gesendet, wenn eine POP3-Nachricht blockiert wurde.



Bild 16 Anpassungen: Blockierte POP3-Proxy-Nachricht

4.9 SNMP

Das *Simple Network Management Protocol* (SNMP) wird dazu benutzt, Netzwerkelemente wie Router, Server oder Switches von einer zentralen Station aus zu überwachen und zu steuern. SNMP ermöglicht es einem Administrator, sich schnell einen Überblick über den Zustand der überwachten Netzwerkgeräte zu verschaffen. Sophos UTM kann so konfiguriert werden, dass sie auf SNMP-Anfragen antwortet oder SNMP-Traps an SNMP-Verwaltungstools sendet.Ersteres wird mithilfe von sogenannten *Management Information Bases* (MIBs) erreicht.

Eine MIB definiert, welche Informationen zu welchen Netzwerkelementen abgerufen werden können. Sophos UTMunterstützt SNMP Version 2 und 3 sowie die folgenden MIBs:

- **DISMAN-EVENT-MIB:** Management Information Base für Ereignisse
- **HOST-RESOURCES-MIB:** Management Information Base für Host-Ressourcen
- **IF-MIB:** Management Information Base für Schnittstellengruppen
- **IP-FORWARD-MIB:** Management Information Base für IP-Übergabetabelle
- **IF-MIB:** Management Information Base für das *Internet Protocol* (IP)
- **NOTIFICATION-LOG-MIB:** Management Information Base für Benachrichtigungsprotokolle
- **RFC1213-MIB:** Management Information Base für die Netzwerkverwaltung von TCP/IP-basiertem Internet: MIB II
- **SNMPv2-MIB:** Management Information Base für das *Simple Network Management Protocol* (SNMP)
- **TCP-MIB:** Management Information Base für das *Transmission Control Protocol* (TCP)
- **UDP-MIB:** Management Information Base für das *User Datagram Protocol* (UDP)

Um Systeminformationen zu Sophos UTM zu erhalten, müssen Sie einen SNMP-Manager verwenden, der zumindest gegen die RFC1213-MIB (MIB II) kompiliert ist.

4.9.1 Anfrage

Auf der Seite *Verwaltung > SNMP > Abfrage* können Sie die Nutzung von SNMP-Abfragen aktivieren.

Um SNMP-Anfragen zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie *SNMP-Anfragen*.**
   Klicken Sie auf den Schieberegler.

   Die Abschnitte *SNMP-Version* und *SNMP-Zugriffskontrolle* können nun bearbeitet werden.

2. **Wählen Sie die SNMP-Version aus.**
   Wählen Sie im Abschnitt *SNMP-Version* aus der Auswahlliste eine Version aus. Für SNMP Version 3 ist Authentifizierung erforderlich.

3. **Wählen Sie die zugelassene Netzwerke aus.**
   Netzwerke im Feld *Zugelassene Netzwerke* dürfen Anfragen an den SNMP-Agenten von Sophos UTM stellen. Beachten Sie, dass der Zugriff immer auf das Leserecht (engl. read-only) beschränkt ist.

   - **Community-String:** Geben Sie bei Nutzung von Version 2 einen Community-String ein. Ein SNMP-Community-String dient als eine Art Kennwort für den Zugriff auf den SNMP-Agenten. Standardmäßig ist „public“ als SNMP-Community-String voreingestellt. Sie können diesen Wert nach Ihren Bedürfnissen ändern.

     Hinweis – Der Community-String darf aus folgenden Zeichen bestehen: (a–z), (A–Z), (0–9), (+), (_), (@), (.), (-), (Leerzeichen).

   - **Benutzername/Kennwort:** Bei Nutzung von Version 3 ist Authentifizierung erforderlich. Geben Sie einen Benutzernamen und ein Kennwort ein (zweites Mal zur Bestätigung), damit der Remote-Administrator Anfragen versenden kann. Das Kennwort muss mindestens acht Zeichen lang sein. SNMP v3 setzt für die Authentifizierung SHA und für die Verschlüsselung AES ein. Beachten Sie, dass Benutzername/Kennwort für beides verwendet werden.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Darüber hinaus können Sie zusätzliche Informationen zur UTM angeben.

Geräteinformationen

Mit den Eingabefeldern im Abschnitt *Geräteinformationen* können Sie die UTM näher erläutern, z. B. durch Angabe eines Gerätenamens, des Standorts oder des zuständigen Administrators. Diese Informationen können von SNMP-Verwaltungsprogrammen gelesen werden und helfen bei der Identifikation der UTM.

Hinweis – Beachten Sie, dass der gesamte SNMP-Datenverkehr (Protokollversion 2) zwischen der UTM und den *Zugelassenen Netzwerken* unverschlüsselt erfolgt und bei einem Transfer über öffentliche Netze mitgelesen werden kann.

Sophos UTMNotifier MIB

In diesem Abschnitt können Sie den Sophos UTM Notifier MIB herunterladen, der die Definitionen der Sophos UTM SNMP-Benachrichtigungen enthält, die auf Ihren aktuellen

Einstellungen für Benachrichtigungs-Traps basieren.

4.9.2 Traps

Auf der Registerkarte *Traps* können Sie einen SNMP-Trap-Server auswählen, an den Benachrichtigungen über relevante Ereignisse auf der UTM per SNMP-Trap verschickt werden können. Beachten Sie, dass spezielle SNMP-Überwachungssoftware benötigt wird, um die Traps anzeigen zu können.

Die als SNMP-Traps verschickten Nachrichten enthalten einen sogenannten Object Identifier (Objektidentifizierungsnummer) (OID), z. B. `.1.3.6.1.4.1.9789`, der zu den privaten Unternehmensnummern gehört, die von der IANA vergeben werden.Dabei ist `.1.3.6.1.4.1` der Präfix, der für `iso.org.dod.internet.private.enterprise` steht, während `9789` die *private Unternehmensnummer* der Astaro GmbH & Co. KG ist. Die OID für Benachrichtigungen ist `1500`, an die wiederum die OIDs des Benachrichtigungstyps und die des dazugehörigen Fehlercodes (`000-999`) angehängt werden. Die folgenden Benachrichtigungstypen sind verfügbar:

- `DEBUG = 0`
- `INFO = 1`
- `WARN = 2`
- `CRIT = 3`

Beispiel: Die Benachrichtigung „INFO-302: New firmware Up2Date installed“ verwendet die OID `.1.3.6.1.4.1.9789.1500.1.302` und bekommt die folgende Bezeichnung zugewiesen:

```
[<HOST>][INFO][302]
```

Beachten Sie, dass `<HOST>` ein Platzhalter für den Hostnamen darstellt und dass nur Typ und Fehlercode aus der Betreffzeile der Benachrichtigung übermittelt werden.

Um einen SNMP-Trap-Server auszuwählen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Neuer SNMP-Trap-Server*.**
   Das Dialogfeld *Neuen SNMP-Trap-Server erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Host: Die Host-Definition für den SNMP-Trap-Server.

Community-String: Ein SNMP-Community-String dient als eine Art Kennwort für den Zugriff auf die Abfrage von SNMP-Nachrichten. Standardmäßig ist „public“ als SNMP-Community-String voreingestellt. Geben Sie hier den Community-String ein, der auf dem SNMP-Trap-Server konfiguriert ist.

> **Hinweis –** Der Community-String darf aus folgenden Zeichen bestehen: (a–z), (A–Z), (0–9), (+), (_), (@), (.), (-), (Leerzeichen).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Der neue SNMP-Trap-Server wird auf der Registerkarte *Traps* angezeigt.

4.10 Zentrale Verwaltung

Über das Menü *Zentrale Verwaltung* werden Schnittstellen zu Verwaltungstools konfiguriert, die verwendet werden können, um das Gateway zu überwachen oder aus der Ferne zu verwalten.

4.10.1 Sophos UTM Manager

Sophos UTM Manager (SUM) ist das Sophos-Produkt zur zentralen Verwaltung. Sie können mehrere UTM-Appliances mit einem SUM verbinden, über den eine zentrale Überwachung, Konfiguration und Wartung möglich ist. Wenn sich zum Beispiel ein UTM 9.2 mit einem SUM 4.1 verbindet, schält er in den Legacy-Modus. Backups und up2date-Installationen sind dann weiterhin möglich.

Auf dieser Registerkarte können Sie die Verbindung Ihrer UTM mit einem oder zwei SUMs konfigurieren.

> **Hinweis –** Wenn Sie die MSP-Lizenz nutzen, können folgende Änderungen nur durch den Sophos UTM Manager (SUM) durchgeführt werden: SUM deaktivieren, SUM-Host ändern, Rechte des SUM-Administrators ändern.

Damit Sophos UTM von einem SUM-Server überwacht werden kann, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die SUM-Funktionalität auf der Registerkarte *Sophos UTM Manager*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *SUM-Einstellungen* kann bearbeitet werden.

2. **Geben Sie den *SUM-Host* an.**
   Wählen Sie einen SUM-Server aus, mit dem sich die UTM verbinden soll, oder fügen Sie einen hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   - **Authentifizierung** (optional): Wenn der SUM-Server Authentifizierung erfordert, wählen Sie diese Option und geben Sie das Kennwort (vereinbarter Schlüssel) an, das auf dem SUM-Server konfiguriert ist.
   - **SUM-Server als Up2Date-Cache verwenden** (optional): Up2Date-Pakete können von einem Zwischenspeicher (engl. cache) geholt werden, der sich auf dem SUM-Server befindet. Wenn Sie diese Funktionalität für Ihr Gateway verwenden wollen, wählen Sie die Option *SUM-Server als Up2Date-Cache verwenden*. Bitte stellen Sie sicher, dass auf dem SUM-Server, der Ihr Gerät verwaltet, die Up2Date-Cache-Funktionalität ebenfalls aktiv ist. Beachten Sie, dass die Verwendung der Up2Date-Cache-Funktionalität und eines übergeordneten Proxy für Up2Date-Pakete sich gegenseitig ausschließen.

3. **Legen Sie die Berechtigungen des SUM-Administrators fest.**
   Der für die UTM zuständige Administrator kann im SUM nur die Bereiche der UTM verwalten, für die hier eine ausdrückliche Berechtigung erteilt ist. Die hier aufgelisteten Berechtigungen entsprechen dem Hauptmenü und den Verwaltungsoptionen des SUM Gateway Manager.

   Administration: Bei Auswahl kann der Administrator die Funktionen in den Menüs *Wartung* und *Verwaltung* verwenden. Dadurch lässt sich beispielsweise der Bestand anzeigen. Außerdem können Backups erstellt und wiederhergestellt sowie geplante Vorgänge wie Firmware-Aktualisierungen durchgeführt werden.

   Berichte: Bei Auswahl kann der Administrator die Funktionen im *Berichtsmenü* verwenden. Er kann z. B. UTM-Berichte anfordern.

   Überwachung: Bei Auswahl wird die UTM auf den Seiten *Überwachung* angezeigt und der Administrator kann die entsprechenden Funktionen verwenden.

Konfiguration: Bei Auswahl kann der Administrator die Funktionen im *Konfigurationsmenü* verwenden. Er kann der UTM beispielsweise Objekte (Netzwerke, Hosts, VPNs) zuweisen.

Hinweis – Weitere Informationen finden Sie im Administratorhandbuch von Sophos UTM Manager.

4. **Klicken Sie auf *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

Die UTM versucht nun, eine Verbindung zum Sophos UTM Manager aufzubauen. Sobald eine Verbindung zwischen den beiden Systemen existiert, wird der Verbindungsstatus grün. Die UTM kann dann vom hier gewählten SUM-Server überwacht und verwaltet werden. Den aktuellen Verbindungsstatus und den Zustand können Sie im Bereich *SUM-Zustand* verfolgen. Ein Neuladen der Seite aktualisiert diese Daten. Nutzen Sie die Schaltfläche *Live-Protokoll öffnen* und lesen Sie die angezeigten Meldungen sorgfältig, um gegebenenfalls Verbindungsprobleme feststellen zu können.

Einstellungen für einen zweiten SUM

In diesem Abschnitt können Sie optional einen weiteren SUM hinzufügen.Das ist sinnvoll, wenn Sie beispielsweise die Konfiguration selbst vornehmen (erster SUM-Server), aber Ihre Rechner dennoch von einem Dritten überwachen lassen wollen, z. B. Ihrem MSSP (zweiter SUM-Server). Die Einstellungen sind fast identisch mit denen des ersten SUM-Servers, lediglich die Option *Konfiguration* fehlt, da diese nur dem ersten SUM-Server zur Verfügung steht.

Hinweis – Beachten Sie, dass das Gateway und der SUM-Server über Port `4433` miteinander kommunizieren, wohingegen der Zugriff auf den Sophos UTM Manager mit einem Browser über das HTTPS-Protokoll auf Port `4444` für die WebAdmin- und auf Port `4422` für die Gateway-Manager-Schnittstelle erfolgt.

SUM-Zustand

Sie können den aktuellen Verbindungsstatus und Zustand im Abschnitt *SUM-Zustand* sehen. Ein Neuladen der Seite aktualisiert diese Daten.

SUM-Objekte

Dieser Abschnitt ist deaktiviert (ausgegraut), es sei denn, es gibt Objekte, die von einem SUM aus angelegt wurden und dieser SUM ist nun getrennt von der Sophos UTM. SUM-erzeugte

Objekte können u. a. Netzwerkdefinitionen, Definitionen entfernter Hosts und IPsec-VPN-Tunnel sein.

Die Schaltfläche *Objekte aufräumen* kann angeklickt werden, um alle Objekte freizugeben, die von dem SUM angelegt wurden, mit dem das System ehemals verwaltet wurde. Diese Objekte sind normalerweise gesperrt und können auf dem lokalen Gerät nur angeschaut werden. Nach Betätigung der Schaltfläche werden die Objekte voll zugänglich und können vom lokalen Administrator wiederverwendet oder gelöscht werden.

Hinweis – Wenn ehemalige SUM-erzeugte Objekte aufgeräumt werden, können sie nicht zurückverwandelt werden, wenn das Gerät wieder mit demselben SUM verbunden wird.Das heißt, wenn ein entfernter SUM noch Objektdefinitionen für ein Gerät bereithält, das sich später wieder mit ihm verbindet, so werden diese Objekte erneut auf das Gerät übertragen – obwohl dann bereits lokale Kopien existieren.

Live-Protokoll

Sie können das Live-Protokoll verwenden, um die Verbindung zwischen Sophos UTM und dem SUM zu beobachten.Klicken Sie auf die Schaltfläche *Live-Protokoll öffnen*, um das Live-Protokoll in einem neuen Fenster zu öffnen.

4.11 High Availabilty (Hochverfügbarkeit)

In den allermeisten Fällen ist ein Hardware-Fehler für den Ausfall eines Internetsicherheitssystems verantwortlich. Die Fähigkeit eines Systems, bei Ausfall einer seiner Komponenten uneingeschränkten Betrieb zu gewährleisten, wird auch Failover bzw. Hochverfügbarkeit genannt (HA, High-Availability). Sophos UTM bietet Hochverfügbarkeit, indem es ermöglicht, ein redundantes Hot-Standby-System zu konfigurieren, das im Falle eines technischen Versagens des Primärsystems dessen Aufgaben übernimmt (aktiv-passiv). Alternativ dazu können Sie Sophos UTM als Cluster konfigurieren, der speziellen Datenverkehr auf mehrere Maschinen verteilt (aktiv-aktiv), wie man es von konventionellen Lösungen zur Lastverteilung kennt. Das führt zu optimaler Ressourcenauslastung und verringert Rechenzeit.

Die Konzepte *Hochverfügbarkeit* und *Cluster* ähneln sich hinsichtlich ihrer Implementierung in Sophos UTM sehr. So kann z. B. ein hochverfügbares System als ein Zwei-Knoten-Cluster angesehen werden, was die Mindestanforderung an ein redundantes System darstellt.

Jeder Knoten innerhalb eines Clusters kann eine der folgenden Rollen annehmen:

- **Master:** Das Primärsystem in einem Hot-Standby-/Cluster-Aufbau. Innerhalb eines Clusters sorgt der Master für die Synchronisierung und Verteilung der Daten.
- **Slave:** Das Sekundärsystem in einem Hot-Standby-/Cluster-Aufbau, das den Betrieb sicherstellt, falls das Primärsystem ausfällt.
- **Worker:** Ein einfacher Cluster-Knoten, der nur für die Datenverarbeitung zuständig ist.

Alle Knoten überwachen sich gegenseitig mit Hilfe eines sogenannten Heartbeat-Signals, ein in periodischen Abständen verschicktes Multicast-UDP-Datenpaket, um festzustellen, ob die anderen Knoten noch „am Leben" sind (daher der Begriff Heartbeat, dt. Herzschlag).Falls aufgrund eines technischen Fehlers einer der Knoten kein Heartbeat-Signal mehr aussenden kann, wird er als *tot* betrachtet. Je nach der Rolle, die der ausgefallene Knoten innehatte, ändert sich die Konfiguration des Aufbaus wie folgt:

- Falls der Master-Knoten ausfällt, übernimmt der Slave-Knoten seinen Platz und der Worker-Knoten mit der höchsten ID wird Slave.
- Falls der Slave-Knoten ausfällt, wird der Worker-Knoten mit der höchsten ID zum Slave.
- Falls ein Worker-Knoten ausfällt, bemerken Sie im Höchstfall Leistungseinbußen aufgrund der verringerten Rechenleistung. Die Ausfallsicherheit ist dadurch nicht beeinträchtigt.

Berichte

Alle Berichtsdaten werden auf dem Master-Knoten konsolidiert und in Abständen von fünf Minuten auf die anderen Knoten übertragen. Im Fall einer Übernahme durch das Sekundärsystem verlieren Sie daher höchstens fünf Minuten an Daten. Es gibt allerdings einen Unterschied hinsichtlich der Zusammenfassung der Daten. Die Diagramme auf den Registerkarten *Protokolle & Berichte* > *Hardware* repräsentieren lediglich die Daten des Knotens, der gerade Master ist. Netzwerkverkehrsdaten wiederum, wie sie beispielsweise auf der Seite *Protokolle & Berichte* > *Netzwerknutzung* angezeigt werden, repräsentieren Daten von allen beteiligten Knoten. So zeigt z. B. das Histogramm der heutigen CPU-Auslastung die aktuelle Prozessorauslastung des Master-Knotens. Im Fall einer Übernahme durch den Slave wären dies dann die Daten des Slave. Im Gegensatz dazu enthalten z. B. die Informationen über die häufigsten Netzwerkdienste die Daten aller Knoten, die bei der verteilten Verarbeitung des Datenverkehrs involviert waren.

Hinweise

- Das *Address Resolution Protocol* (ARP) wird nur vom tatsächlichen Master benutzt, d. h. Slave- und Worker-Knoten senden und beantworten keine ARP-Anfragen.
- Im Fall einer Übernahme führt die Einheit, die die Aufgaben übernimmt, eine ARP-Bekanntgabe (auch bekannt als *gratuitous ARP*) durch. Gewöhnlich dient diese ARP-Anfrage dazu, den ARP-Cache der Hosts, die diese Anfrage erhalten, zu aktualisieren. Die ARP-Bekanntgabe wird dazu benutzt, bekannt zu geben, dass die IP-Adresse des Masters auf den Slave übertragen wurde.
- Alle Schnittstellen, die auf dem Master konfiguriert sind, müssen eine physikalische Verbindung haben, das heißt, der Port muss korrekt mit einem Netzwerkgerät verbunden sein.

4.11.1 Hardware- und Software-Voraussetzungen

Die folgenden Hardware- und Software-Voraussetzungen müssen für die HA- und Cluster-Funktionalität erfüllt sein:

- Gültige Lizenz mit aktivierter HA-Option (für das Standby-Gerät benötigen Sie lediglich eine zusätzliche Basislizenz).
- Zwei UTM-Geräte mit identischer Software-Version und identischer Hardware oder zwei UTM-Appliances des gleichen Modells.
- Heartbeat-fähige Ethernet-Netzwerkkarten. Auf der HCL (Hardware Compatibility List) können Sie nachsehen, welche Netzwerkkarten unterstützt werden. Die HCL befindet sich in der SophosKnowledgebase (verwenden Sie „HCL“ als Suchbegriff).
- Ethernet-Crosskabel (für die Verbindung zwischen Master und Slave in einem Hot-Standby-System). UTM Appliances der Modelle 320, 425 und 525, deren dedizierte HA-Schnittstelle eine Gigabit-auto-MDX-Schnittstelle ist, können auch durch ein Standard-Ethernetkabel der IEEE-Norm 802.3 miteinander verbunden werden.
- Netzwerk-Switch (um Cluster-Knoten miteinander zu verbinden).

4.11.2 Status

Die Registerkarte *Verwaltung* > *Hochverfügbarkeit* > *Status* führt alle Geräte auf, die zu einem Hot-Standby-System bzw. Cluster gehören, und zeigt die folgenden Informationen an:

- **ID:** Die Knoten-ID des Geräts.In einem Hot-Standby-System ist die ID entweder `1` (Master) oder `2` (Slave).
  Die ID in einem Cluster reicht von 1 bis 10, da ein Cluster aus maximal zehn Knoten bestehen kann.
- **Rolle:** Jeder Knoten innerhalb eines Clusters kann eine der folgenden Rollen annehmen:
  - MASTER: Das Primärsystem in einem Hot-Standby-/Cluster-Aufbau. Innerhalb eines Clusters sorgt der Master für die Synchronisierung und Verteilung der Daten.
  - SLAVE: Das Sekundärsystem in einem Hot-Standby-/Cluster-Aufbau, das den Betrieb sicherstellt, falls das Primärsystem ausfällt.
  - WORKER: Ein einfacher Cluster-Knoten, der nur für die Datenverarbeitung zuständig ist.
- **Gerätename:** Der Name des Geräts.
- **Status:** HA-Status des Knotens. Die folgenden Werte sind möglich:
  - AKTIV: Der Knoten ist voll funktionsfähig.
  - NICHT VERBUNDEN: Eine oder mehrere Schnittstellen sind nicht verbunden.
  - UP2DATE: Auf dem Knoten wird gerade ein Up2Date ausgeführt.
  - UP2DATE FEHLGESCHLAGEN: Das Up2Date auf dem Knoten ist fehlgeschlagen.
  - TOT: Der Knoten ist nicht erreichbar.
  - SYNCING: Die Datensynchronisierung läuft. Dieser Status wird angezeigt, wenn ein Übernahmevorgang stattfindet. Die anfängliche Synchronisierungszeit beträgt mindestens fünf Minuten. Sie kann jedoch durch alle an der Synchronisierung beteiligten Programme verlängert werden. Während ein SLAVE synchronisiert und sich im Zustand *SYNCING* befindet, findet keine Übernahme, z. B. wegen eines Linkausfalls auf dem Master-Knoten, statt.
- **Version:** Versionsnummer der Sophos UTM Software, die auf dem System installiert ist.
- **Letzte Statusänderung:** Zeitpunkt der letzten Statusänderung.

Neustart/Herunterfahren: Mit diesen Schaltflächen kann ein Gerät manuell neu gestartet oder heruntergefahren werden.

Knoten entfernen: Verwenden Sie diese Schaltfläche, um einen toten Cluster-Knoten über WebAdmin zu entfernen. Alle knotenspezifischen Daten wie E-Mail-Quarantäne und Spool werden dann vom Master übernommen.

Klicken Sie auf die Schaltfläche *HA-Live-Protokoll öffnen* in der rechten oberen Ecke, um das Hochverfügbarkeits-Live-Protokoll in einem separaten Fenster zu öffnen.

4.11.3 Systemstatus

Die Registerkarte *Verwaltung > Hochverfügbarkeit > Systemstatus* führt alle Geräte auf, die zu einem Hot-Standby-System bzw. Cluster gehören, und zeigt Informationen über die Ressourcennutzung jedes einzelnen Gerätes an:

- Die CPU-Auslastung in Prozent
- Die RAM-Auslastung in Prozent
- Der von der Swap-Partition genutzte Festplattenplatz in Prozent
- Der von der Protokollpartition (engl. log partition) belegte Festplattenplatz in Prozent
- Der von der Datenpartition belegte Festplattenplatz in Prozent
- Der Status des USV-Gerätes (unterbrechungsfreie Stromversorgung) (falls vorhanden)

4.11.4 Konfiguration

Die HA-Funktionalität von Sophos UTM umfasst drei Grundeinstellungen:

- Aus
- Automatische Konfiguration
- Hot-Standby (aktiv-passiv)
- Cluster (aktiv-aktiv)

Automatische Konfiguration: Sophos UTM verfügt über eine Plug-and-Play-Konfigurationsoption speziell für UTM-Appliances, die es ermöglicht, ein Hot-Standby-System bzw. einen Cluster aufzubauen, ohne jedes Gerät, das zum Cluster hinzugefügt werden soll, einzeln konfigurieren oder manuell installieren zu müssen. Dazu verbindet man einfach die HA-Schnittstellen (`eth3`) der UTM-Appliances miteinander und wählt auf allen Geräten jeweils die Option *Automatische Konfiguration*.

Hinweis – Damit die *Automatische Konfiguration* funktioniert, müssen alle UTM-Appliances vom gleichen Modell sein. Sie können z. B. nur zwei UTM-320-Appliances zum Aufbau eines HA-Systems verwenden; eine UTM 220 kann hingegen nicht mit einer UTM 320 kombiniert werden.

Wenn Sie zwei UTM-Appliances über die entsprechende Schnittstelle miteinander verbinden, erkennen sich alle Geräte gegenseitig und konfigurieren sich selbstständig als HA-System. Das Gerät mit der längeren Betriebszeit wird Master. Im unwahrscheinlichen Fall, dass die Betriebszeit identisch ist, wird die Entscheidung, welches Gerät Master werden soll, anhand der MAC-Adresse getroffen.

Wenn Sie UTM Software verwenden, wird die Option *Automatische Konfiguration* auf dedizierten Slave-Systemen dazu benutzt, automatisch einem Master- oder bereits konfigurierten Hot-Standby-System bzw. Cluster beizutreten. Aus diesem Grund ist *Automatische Konfiguration* eher als Übergangsmodus zu verstehen denn als eigenständiger HA-Betriebsmodus. Denn der HA-Betriebsmodus ändert sich in *Hot-Standby* oder *Cluster*, sobald das Gerät mit der Einstellung *Automatische Konfiguration* einem Hot-Standby-System bzw. Cluster beitritt. Voraussetzung dafür allerdings ist, dass die Option *Automatische Konfiguration neuer Geräte aktivieren* auf dem Master aktiviert ist. Diese Funktion sorgt dafür, dass genau die Geräte automatisch einem Hot-Standby-System bzw. Cluster hinzugefügt werden, deren HA-Betriebsmodus auf *Automatische Konfiguration* steht.

Hot-Standby (aktiv-passiv): Sophos UTM kann als Hot-Standby-System, bestehend aus zwei Knoten, konfiguriert werden, was die Mindestvoraussetzung für ein redundantes System ist. Eine der größten technischen Verbesserungen der Sophos UTM Software 9 ist, dass die Latenzzeit für eine Übernahme durch das Standby-Gerät auf weniger als zwei Sekunden verringert werden konnte. Zusätzlich zur Firewall-Synchronisierung bietet das Gateway auch eine IPsec-Tunnel-Synchronisierung. Dies bedeutet, dass weder Road-Warrior- noch entfernte VPN-Gateway-Verbindungen nach einer Übernahme neu aufgebaut werden müssen. Objekte, die sich in Quarantäne befinden, werden ebenfalls synchronisiert und sind so auch nach einem Ausfall des Primärsystems noch verfügbar.

Cluster (aktiv-aktiv): (nicht verfügbar mit BasicGuard-Abonnement): Um der steigenden Nachfrage nach der Verarbeitung von großen Mengen an Internetverkehr in Echtzeit gerecht zu werden, kann Sophos UTM als Cluster konfiguriert werden. Ein Cluster besteht aus mehreren Knoten, auf die rechenintensive Aufgaben wie z. B. Inhaltsfilterung, Virenscans, Angriffsschutz und Entschlüsselung gleichmäßig verteilt werden können. Ohne die Notwendigkeit eines

speziellen Lastenausgleichsprogramms wird so die Gesamtleistung des Gateways deutlich erhöht.

Hinweis – Wenn Sie einen Cluster konfigurieren, stellen Sie sicher, dass Sie den Master zuerst konfigurieren, bevor Sie die anderen Geräte mit dem Switch verbinden.

Die Einrichtung von Master, Slaves und Workers unterscheidet sich nur in wenigen Punkten. Gehen Sie folgendermaßen vor:

1. **Wählen Sie einen HA-Betriebsmodus.**
   Standardmäßig ist die HA-Funktion deaktiviert. Die folgenden Modi sind möglich:
   - Automatische Konfiguration
   - Hot-Standby (aktiv-passiv)
   - Cluster (aktiv-aktiv)

   Hinweis – Falls Sie den Betriebsmodus später ändern möchten, müssen Sie vorher den Modus auf *Aus* stellen. Erst danach können Sie einen der Betriebsmodi *Automatische Konfiguration*, *Hot-Standby* oder *Cluster* wählen.

   Note – Wenn die Lizenz / das Abonnement abgelaufen oder nicht vorhanden ist, kann der Betriebsmodus nur auf *Aus* und dem aktuellen Betriebsmodus geändert werden.

   Abhängig von Ihrer Auswahl werden eine oder mehrere Optionen angezeigt.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Sync-NIC: Wählen Sie die Netzwerkkarte aus, über die Master- und Slave-Systeme miteinander kommunizieren. Wenn Linkbündelung aktiviert ist, können Sie hier auch eine Linkbündelungsschnittstelle sehen.

   Hinweis – Beachten Sie, dass nur jene Schnittstellen angezeigt werden, die noch nicht konfiguriert wurden. Es ist möglich, die Synchronisierungsschnittstelle in einer laufenden Konfiguration zu ändern. Beachten Sie, dass danach alle Knoten einen Neustart durchführen werden.

   Die folgenden Optionen können nur konfiguriert werden, wenn entweder *Hot-Standby* oder *Cluster* als Betriebsmodus ausgewählt wurde:

Gerätename: Geben Sie einen aussagekräftigen Namen für das Gerät ein.

Geräteknoten-ID: Weisen Sie dem Gerät eine Knoten-ID zu. Im Fall eines Ausfalls des Primärsystems wird der Knoten mit der höchsten ID Master.

Verschlüsselungsschlüssel: Das Kennwort, mit dem die Kommunikation zwischen Master und Slave verschlüsselt wird (zur Sicherheit müssen Sie das Kennwort zweimal eingeben). Der Schlüssel darf maximal 16 Zeichen lang sein.

3. **Klicken Sie auf *Übernehmen*.**
   Die Konfiguration der HA-Ausfallsicherheit auf dem Gerät ist damit abgeschlossen.

Das Gateway im Hot-Standby-Modus wird in regelmäßigen Abständen über die Sync-NIC (Synchronisierungsschnittstelle) aktualisiert. Sollte das Primärsystem ausfallen, wird das Sekundärsystem unmittelbar in den normalen Modus wechseln und die Aufgaben des Primärsystems übernehmen.

Hinweis – Wenn Sie ein Hot-Standby-System bzw. einen Cluster deaktivieren, führen die Slave- und Worker-Knoten eine Werkszurücksetzung durch und fahren herunter.

Weitere Informationen zu diesem Thema (insbesondere Anwendungsfälle) finden Sie im *HA/Cluster Guide* in der Sophos-Knowledgebase.

Erweitert

In diesem Abschnitt können Sie einige erweiterte Einstellungen vornehmen.

Automatische Konfiguration neuer Geräte aktivieren: Wenn Sie ein Hot-Standby-System bzw. Cluster manuell konfiguriert haben, sorgt diese Option dafür, dass genau die Geräte automatisch zu einem Hot-Standby-System bzw. Cluster hinzugefügt werden, deren HA-Betriebsmodus auf *Automatische Konfiguration* steht. Da diese Option jedoch keinen Effekt auf Slave-Systemen hat, können Sie die Option aktiviert lassen, was der Standardeinstellung entspricht.

Knoten während Up2Date reservieren: Aktivieren Sie diese Option, damit während eines Updates auf eine neue Systemversion die Hälfte der HA/Cluster-Knoten die aktuelle Systemversion beibehält. Sobald die neue Version stabil ist, können Sie die verbleibenden Knoten auf der Seite *Verwaltung > Hochverfügbarkeit > Status* aktualisieren. Falls die neue Version einen Ausfall der aktualisierten Knoten zur Folge hat, bilden die verbleibenden Knoten einen neuen HA/Cluster mit der alten Version. Anschließend können Sie auf den nicht mehr funktionierenden Knoten wieder die alte Version installieren oder auf das nächste Update warten.

Wenn *Knoten während Up2Date zurückhalten* aktiv ist, werden reservierte Knoten nach einem Update nicht mehr synchronisiert, da die Synchronisation nur funktioniert, wenn Knoten die gleiche Systemversion besitzen. Stattdessen wird der Status der reservierten Knoten erhalten. Wenn Sie daher aus irgendeinem Grund die reservierten Knoten reaktivieren, sind alle Konfigurationsänderungen und Berichtsdaten aus der Zeit zwischen Updatebeginn und Reaktivierung verloren.

Preferred Master: Hier können Sie einen designierten Master-Knoten bestimmen, indem Sie einen Knoten von der Auswahlliste wählen. Im Fall einer Übernahme wird der gewählte Knoten nicht im Slave-Modus bleiben, nachdem die Verbindung wiederhergestellt ist, sondern in den Master-Modus zurückkehren.

Backup-Schnittstelle: Um zu verhindern, dass sowohl Master als auch Slave gleichzeitig Master werden (Master-Master-Situationen), beispielsweise durch ein Versagen der HA-Synchronisierungsschnittstelle oder das Abziehen eines Netzwerkkabels, kann eine Heartbeat-fähige Backup-Schnittstelle ausgewählt werden. Diese zusätzliche Heartbeat-fähige Schnittstelle kann eine beliebige konfigurierte und aktive Ethernet-Schnittstelle sein. Wenn eine Backup-Schnittstelle gewählt wurde, wird ein zusätzliches Heartbeat-Signal über diese Schnittstelle in eine Richtung vom Master zum Slave gesendet, um sicherzustellen, dass die Master-Slave-Konfiguration intakt bleibt. Wenn die Master-Slave-Verbindung deaktiviert ist und die Backup-Schnittstelle aktiv wird, erhält der Administrator eine Benachrichtigung, die ihn darüber informiert, dass einer der Cluster-Knoten tot ist. Da diese Option jedoch keinen Effekt auf Slave-Systeme hat, können Sie sie unkonfiguriert lassen.

Hinweis – Wenn die HA-Synchronisierungsschnittstelle ausfällt, wird keine Konfiguration mehr synchronisiert. Die Backup-Schnittstelle verhindert lediglich Master-Master-Situationen.

4.12 Ausschalten/Neustart

Auf dieser Registerkarte können Sie die Sophos UTM manuell herunterfahren oder neu starten.

Herunterfahren: Mit dieser Aktion können Sie das System herunterfahren und alle Dienste ordnungsgemäß stoppen. Falls Sie keinen Monitor oder LCD-Display angeschlossen haben, wird das erfolgreiche Herunterfahren durch eine endlose Reihe von Pieptönen im Abstand von einer Sekunde signalisiert.

Um die Sophos UTM herunterzufahren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *System jetzt herunterfahren*.**
2. **Bestätigen Sie den Warnhinweis.**
   Bestätigen Sie die Sicherheitsabfrage „System wirklich herunterfahren?" mit *OK*.

   Das System fährt anschließend herunter.

Abhängig von der verwendeten Hardware und Konfiguration kann dieser Prozess mehrere Minuten dauern. Sie sollten das Gerät erst dann ausschalten, nachdem es vollständig heruntergefahren ist. Wenn Sie das Gerät vorher ausschalten, wird das System beim nächsten Start den Zustand des Dateisystems überprüfen, was den Startvorgang erheblich verzögert. Im schlimmsten Fall können Daten verloren gehen.

Einen erfolgreichen Systemstart signalisiert das Gerät mit fünf aufeinanderfolgenden Pieptönen.

Neustart: Mit dieser Aktion können Sie das System neu starten. Abhängig von der verwendeten Hardware und Konfiguration kann dieser Prozess mehrere Minuten dauern.

Um die Sophos UTM neu zu starten, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *System jetzt neu starten*.**
2. **Bestätigen Sie den Warnhinweis.**
   Bestätigen Sie die Sicherheitsabfrage „System wirklich neu starten?" mit *OK*.

   Das System fährt herunter und startet anschließend neu.

5 Definitionen & Benutzer

In diesem Kapitel wird die Konfiguration von Netzwerk-, Dienst- und Zeitraumdefinitionen beschrieben, die von Sophos UTM verwendet werden.Die *Definitionenübersicht* im WebAdmin zeigt die Anzahl aller Netzwerkdefinitionen nach Typ und die Anzahl aller Dienstdefinitionen nach Protokolltyp.

Die Seiten des Menüs *Definitionen & Benutzer* ermöglichen die zentrale Definition von Netzwerken und Diensten, die dann überall in den Konfigurationsmenüs verwendet werden können. Dies erlaubt es Ihnen, überall mit einheitlichen Namen zu arbeiten, anstatt mit uneingängigen IP-Adressen, Portnummern und Netzmasken. Ein weiterer Vorteil von Definitionen liegt darin, dass Sie einzelne Netzwerke und Dienste gruppieren und dadurch auf einmal konfigurieren können. Wenn Sie dann beispielsweise später Änderungen an den Einstellungen dieser Gruppe vornehmen, gelten diese für alle darin enthaltenen Netzwerke und Dienste.

Zudem beschreibt dieses Kapitel die Konfiguration von Benutzerkonten, Benutzergruppen und externen Authentifizierungsservern von Sophos UTM sowie die Authentifizierung für Client-PCs.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Netzwerkdefinitionen
- Dienstdefinitionen
- Zeitraumdefinitionen
- Benutzer & Gruppen
- Client-Authentifizierung
- Authentifizierungsdienste

5.1 Netzwerkdefinitionen

Im Menü *Definitionen & Benutzer > Netzwerkdefinitionen* werden die Hosts, Netzwerke und Netzwerkgruppen sowie MAC-Adressdefinitionen festgelegt. Die hier angelegten Definitionen können in vielen anderen WebAdmin-Konfigurationen verwendet werden.

5.1.1 Netzwerkdefinitionen

Auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* werden die Hosts, Netzwerke und Netzwerkgruppen der UTM festgelegt. Die hier angelegten Definitionen können an vielen anderen Stellen der WebAdmin-Konfigurationsmenüs verwendet werden.

Beim Öffnen der Registerkarte werden standardmäßig alle Netzwerkdefinitionen angezeigt. Mit Hilfe der Auswahlliste oberhalb der Liste können Sie die angezeigte Auswahl auf Netzwerkdefinitionen mit bestimmten Eigenschaften einschränken.

Tipp – Durch einen Klick auf das Infosymbol einer Netzwerkdefinition in der Liste *Netzwerkdefinitionen* können Sie alle Konfigurationsoptionen sehen, in denen diese Netzwerkdefinition verwendet wird.

Die Netzwerktabelle enthält auch statische Netzwerke, die automatisch vom System angelegt wurden und die weder bearbeitet noch gelöscht werden können:

- **Schnittstellen-Adresse:** Eine Definition dieser Art wird für jede Netzwerkkarte hinzugefügt.Sie enthält die aktuelle IP-Adresse der Schnittstelle. Ihr Name besteht aus dem Namen der Schnittstelle, gefolgt von dem Zusatz „(Address)“.
- **Schnittstellen-Broadcast-Adresse:** Eine Definition dieser Art wird für jede Ethernet-artige Netzwerkschnittstelle hinzugefügt. Sie enthält die aktuelle IPv4-Broadcast-Adresse der Schnittstelle. Ihr Name besteht aus dem Namen der Schnittstelle, gefolgt von dem Zusatz „(Broadcast)“.
- **Schnittstellen-Netzwerkadresse:** Eine Definition dieser Art wird für jede Ethernet-artige Netzwerkschnittstelle hinzugefügt. Sie enthält das aktuelle IPv4-Netzwerk der Schnittstelle. Ihr Name besteht aus dem Namen der Schnittstelle, gefolgt von dem Zusatz „ (Network)“.
- **Internet (IPv4/IPv6):** Eine Netzwerkdefinition (jeweils für IPv4 und IPv6, falls IPv6 aktiviert ist), die an diejenige Schnittstelle gebunden ist, die als Standardgateway fungiert. Die Benutzung dieser Definition sollte Ihren Konfigurationsprozess erleichtern. Wenn die Uplink-Ausgleich-Funktion aktiviert ist, ist die Definition *Internet* an die *Uplink-Schnittstellen* gebunden.

Hinweis – Benutzernetzwerkobjekte, die über die Client-Authentifizierung authentifiziert sind, werden aus Leistungsgründen immer als nicht aufgelöst (unresolved) angezeigt.

Um eine Netzwerkdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Netzwerkdefinitionen* auf *Neue Netzwerkdefinition*.**
   Das Dialogfeld *Neue Netzwerkdefinition erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   (Abhängig von dem gewählten Definitionstyp werden weitere Parameter der Netzwerkdefinition angezeigt.)

   Name: Geben Sie einen aussagekräftigen Namen für diese Definition ein.

   Art: Wählen Sie den Typ der Netzwerkdefinition. Die folgenden Typen sind verfügbar:

   - **Host:** Einzelne IP-Adresse.Geben Sie die folgenden Informationen an:
     - **IPv4/IPv6-Adresse:** Die IP-Adresse des Hosts (Sie können keine IP-Adresse einer bereits konfigurierten Schnittstelle eingeben).
     - **DHCP-Einstellungen** (optional): In diesem Bereich können Sie statische Zuordnungen zwischen Hosts und IP-Adresse festlegen. Zu diesem Zweck benötigen Sie einen konfigurierten DHCP-Server (siehe *Netzwerkdienste > DHCP > Server*).

       Hinweis – Um IP-Adresskonflikten zwischen regulär zugeordneten Adressen aus dem DHCP-Pool und statisch zugeordneten Adressen vorzubeugen, stellen Sie sicher, dass die statisch zugeordnete Adresse nicht aus dem DHCP-Pool stammt. Zum Beispiel könnte die statische Zuordnung von `192.168.0.200` darin resultieren, dass zwei Systeme dieselbe IP-Adresse erhalten, wenn der DHCP-Pool `192.168.0.100` – `192.168.0.210` umfasst.

       IPv4 DHCP: Wählen Sie den IPv4 DHCP-Server, der für die statische Zuordnung verwendet werden soll.

       MAC-Adressen: Geben Sie die MAC-Adresse der Host-Netzwerkkarten ein. MAC-Adressen werden gewöhnlich in sechs Gruppen von je zwei

durch Doppelpunkt getrennte Hexadezimalziffern angegeben (z. B. `00:04:76:16:EA:62`).

IPv6 DHCP: Wählen Sie den IPv6 DHCP-Server, der für die statische Zuordnung verwendet werden soll.

DHCP Unique IDs: Geben Sie die DUIDs der Hosts ein.Bei Windows-Betriebssystemen finden Sie die DUID beispielsweise in der Windows-Registrierungsdatenbank:
`HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters`

Bitte beachten Sie, dass Sie zwei Hexadezimalziffern jeweils durch einen Doppelpunkt trennen müssen, z. B. `00:01:00:01:13:30:65:56:00:50:56:b2:07:51`).

- **DNS-Einstellungen** (optional): Wenn Sie keinen eigenen DNS-Server einrichten wollen, aber statische DNS-Zuordnungen für einige Hosts Ihres Netzwerks benötigen, können Sie diese Zuordnungen in diesem Abschnitt der entsprechenden Hosts angeben. Beachten Sie, dass diese Lösung sich nur für eine begrenzte Anzahl von Hosts eignet und in keiner Weise als Ersatz für einen richtigen DNS-Server dienen kann.
  Hostname: Geben Sie den vollständigen Domänennamen (FQDN, fully qualified domain name) des Hosts ein.

  Reverse-DNS: Markieren Sie dieses Auswahlfeld, um die Zuordnung der IP-Adresse eines Hosts zu seinem Namen zu ermöglichen. Beachten Sie, dass eine IP-Adresse immer nur auf einen Namen verweisen kann, wohingegen mehrere Namen auf die gleiche IP-Adresse verweisen können.

  Zusätzliche Hostnamen: Klicken Sie auf das Plussymbol, um zusätzliche Hostnamen für den Host hinzuzufügen.

- **DNS-Host:** Ein DNS-Hostname, der dynamisch vom System aufgelöst wird, um eine IP-Adresse zu erhalten. DNS-Hosts sind nützlich, wenn es darum geht, mit dynamischen IP-Endpoints zu arbeiten. Das System löst diese Definitionen periodisch immer wieder neu auf, wobei es sich an den TTL-Werten (Time To Live) orientiert, und aktualisiert die Definitionen bei Bedarf mit den neuen IP-Adressen. Geben Sie die folgenden Informationen an:
  - **Hostname:** Der Name des Hosts, der aufgelöst werden soll.

- **DNS-Gruppe:** Eine DNS-Gruppe ähnelt einem DNS-Host, aber sie kann mehrere RRs (Resource Records, dt. Ressourcen-Einträge) für einen einzelnen Host im DNS verarbeiten. Eine DNS-Gruppe ist nützlich zur Definition von Firewallregeln und Ausnahmen in transparenten Proxies.
- **Netzwerk:** Ein Standard-IP-Netzwerk, das aus einer Netzwerkadresse und einer Netzmaske besteht.Geben Sie die folgenden Informationen an:
  - **IPv4/IPv6-Adresse:** Die Netzwerkadresse des Netzwerks (Sie können keine IP-Adresse einer bereits konfigurierten Schnittstelle eingeben).
  - **Netzmaske:** Die Bitmaske, die angibt, wie viele Bit eines Oktetts das Subnetzwerk spezifizieren und wie viele Bit Platz für Hostadressen bieten.
- **Bereich:** Wählen Sie diese Option, um einen ganzen Bereich von IPv4-Adressen zu definieren.Geben Sie die folgenden Informationen an:
  - **IPv4 von:** Die erste IPv4-Adresse des Bereichs.
  - **IPv4 bis:** Die letzte IPv4-Adresse des Bereichs.
  - **IPv6 von:** Die erste IPv6-Adresse des Bereichs.
  - **IPv6 bis:** Die letzte IPv6-Adresse des Bereichs.
- **Multicast-Gruppe:** Ein Netzwerk, das einen festgelegten Multicast-Netzwerkbereich umfasst.
  - **IPv4-Adresse:** Die Netzwerkadresse des Multicast-Netzwerks, die im Bereich `224.0.0.0` bis `239.255.255.255` liegen muss.
  - **Netzmaske:** Die Bitmaske, die angibt, wie viele Bit eines Oktetts das Subnetzwerk spezifizieren und wie viele Bit Platz für Hostadressen bieten.
- **Netzwerkgruppe:** Eine Art Behälter, der eine Liste anderer Netzwerkdefinitionen enthält. Sie können ihn verwenden, um Netzwerke und Hosts zusammenzufassen, damit Ihre Konfiguration übersichtlicher wird.Sobald Sie die *Netzwerkgruppe* ausgewählt haben, erscheint das Feld *Mitglieder*, über das Sie die Gruppenmitglieder hinzufügen können.
- **Verfügbarkeitsgruppe:** Eine Gruppe aus Hosts und/oder DNS-Hosts, die nach Priorität angeordnet sind. Die Verfügbarkeit aller Hosts wird standardmäßig mit ICMP-Pings, die im Abstand von 60 Sekunden erfolgen, überprüft. Der (verfügbare) Host mit der höchsten Priorität wird für die Konfiguration verwendet.Sobald Sie die *Verfügbarkeitsgruppe* ausgewählt haben, erscheint das Feld *Mitglieder*, über das Sie die Gruppenmitglieder hinzufügen können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Die angezeigten Optionen hängen vom oben ausgewählten *Typ* ab.

   Schnittstelle (optional): Die Netzwerkdefinition kann an eine bestimmte Schnittstelle gebunden werden, sodass Verbindungen zu dieser Definition nur über diese Schnittstelle zustande kommen.

   Überwachungstyp (nur beim Typ *Verfügbarkeitsgruppe*): Wählen Sie das Dienstprotokoll für die Verfügbarkeitsprüfung. Wählen Sie für die Dienstüberwachung entweder *TCP* (TCP-Verbindungsaufbau), *UDP* (UDP-Verbindungsaufbau), *Ping* (ICMP-Ping), *HTTP Host* (HTTP-Anfragen) oder *HTTPS Hosts* (HTTPS-Anfragen). Wenn Sie *UDP* verwenden, wird zunächst eine Ping-Anfrage versendet. Ist diese erfolgreich, folgt ein UDP-Paket mit der Payload 0. Ist der Ping erfolglos oder der ICMP-Port nicht erreichbar, gilt der Host als ausgefallen.

   Port (nur beim Überwachungstyp *TCP* oder *UDP*): Nummer des Ports, an den die Anfrage gesendet wird.

   URL (optional, nur bei den Überwachungstypen *HTTP Host* oder *HTTPS Host*): Angefragte URL.Sie können statt den Standard-Ports 80 und 443 auch andere Ports verwenden, indem Sie die Port-Information an die URL anhängen, z. B. `http://beispiel.domaene:8080/index.html`. Wenn keine URL angegeben ist, wird das Wurzelverzeichnis angefragt.

   Intervall: Geben Sie eine Zeitspanne in Sekunden an, in der die Hosts überprüft werden.

   Zeitüberschreitung: Geben Sie die maximale Zeitspanne, in der die Hosts eine Antwort senden können, in Sekunden ein. Wenn ein Host während dieser Zeit nicht antwortet, wird er als tot betrachtet.

   Immer aufgelöst: Diese Option ist vorausgewählt, sodass für den Fall, dass kein Host erreichbar ist, die Gruppe zu jenem Host aufgelöst wird, der zuletzt verfügbar war.Andernfalls, wenn alle Hosts tot sind, wird die Gruppe auf *nicht aufgelöst* gesetzt.

4. **Klicken Sie auf *Speichern*.**
   Die neue Definition wird in der Liste Netzwerke angezeigt.

Um eine Definition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

5.1.2 MAC-Adressdefinitionen

Die Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen > MAC-Adressdefinitionen* ist die zentrale Stelle für die Festlegung von MAC-Adressdefinitionen, d. h. MAC-Adresslisten. Eine MAC-Adressdefinition kann wie eine Netzwerkdefinition verwendet werden. Außerdem kann sie dazu verwendet werden, eine Regel, die auf Hosts/IP-Adressen basiert, auf nur diejenigen Geräte einzuschränken, die eine der festgelegten MAC-Adressen besitzen.

Tipp – Durch einen Klick auf das Infosymbol einer MAC-Adressdefinition können Sie alle Konfigurationsoptionen sehen, in denen diese Definition verwendet wird.

Um eine MAC-Adressdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *MAC-Adressdefinitionen* auf *Neue MAC-Adressliste*.**
   Das Dialogfeld *Neue MAC-Adressliste* öffnet sich.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Definition ein.

   MAC-Adressen: Klicken Sie auf das Plussymbol, um nacheinander einzelne MAC-Adressen hinzuzufügen oder verwenden Sie das Action-Symbol um über Kopieren und Einfügen MAC-Adressen zu importieren. MAC-Adressen werden gewöhnlich in sechs Gruppen von je zwei durch Doppelpunkt getrennte Hexadezimalziffern angegeben (z. B. `00:04:76:16:EA:62`).

   Hosts: Fügen Sie Hosts hinzu, deren MAC-Adressen Sie zur MAC-Adressdefinition hinzufügen möchten. Die MAC-Adressen, die im Bereich *DHCP-Einstellungen* einer Host-Definition festgelegt sind, werden zur MAC-Adressliste hinzugefügt. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Hinweis – Die Anzahl der Adressen pro Adressdefinition ist für die folgenden Anwendungsbereiche begrenzt: Für die Einschränkung des Zugriffs auf ein kabelloses Netzwerk beträgt das Maximum 200. Für die Einschränkung des Zugriffs auf ein RED-Gerät beträgt das Maximum bei RED 10 200 und bei RED 50 400.

Hinweis – Sie können entweder MAC-Adressen oder Hosts oder beides eingeben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Definition wird in der Liste *MAC-Adressdefinitionen* angezeigt.

Um eine MAC-Adressdefinition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

5.2 Dienstdefinitionen

Auf der Seite *Definitionen & Benutzer > Dienstdefinitionen* werden die Dienste und die Dienstgruppen zentral definiert und verwaltet. Dienste sind Definitionen bestimmter Arten von Netzwerkverkehr und bestehen aus einem Protokoll, z. B. TCP oder UDP, und protokollbezogenen Optionen wie Portnummern. Mittels der Dienste können Sie bestimmen, welche Arten von Netzwerkverkehr von der UTM angenommen oder abgelehnt werden.

Tipp – Durch einen Klick auf das Infosymbol einer Dienstdefinition in der Liste *Dienstdefinitionen* können Sie alle Konfigurationsoptionen sehen, in denen diese Dienstdefinition verwendet wird.

Um eine Dienstdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Dienstdefinitionen* auf *Neue Dienstdefinition*.**
   Das Dialogfeld *Neue Dienstdefinition erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   (Abhängig von dem gewählten Definitionstyp werden weitere Parameter der Netzwerkdefinition angezeigt.)

   Name: Geben Sie einen aussagekräftigen Namen für diese Definition ein.

   Definitionstyp: Wählen Sie den Diensttyp aus. Die folgenden Typen sind verfügbar:

   - **TCP:** TCP-Verbindungen (Transmission Control Protocol) verwenden Portnummern von `0` bis `65535`. Verlorene Pakete werden von TCP erkannt und erneut angefragt. Bei einer TCP-Verbindung informiert der Empfänger den

Absender darüber, wenn er ein Paket erfolgreich erhalten hat (verbindungsbezogenes Protokoll). TCP-Sitzungen beginnen mit einem 3-Wege-Handshake, und Verbindungen werden am Ende der Sitzung geschlossen. Geben Sie die folgenden Informationen an:

- **Zielport:** Geben Sie den Zielport ein, entweder als einzelne Portnummer (z. B. `80`) oder als Bereich (z. B. `1024:64000`) mit einem Doppelpunkt als Trennzeichen.
- **Quellport:** Geben Sie den Quellport ein, entweder als einzelne Portnummer (z. B. `80`) oder als Bereich (z. B. `1024:64000`) mit einem Doppelpunkt als Trennzeichen.

- **UDP:** Das UDP-Protokoll (*User Datagram Protocol*) verwendet Portnummern zwischen `0` und `65535` und ist ein zustandsloses (engl. stateless) Protokoll. Da UDP sich keine Zustände merkt, ist es schneller als TCP, vor allem wenn es sich um das Versenden kleiner Datenmengen handelt. Diese Zustandslosigkeit bedeutet aber auch, dass UDP nicht erkennen kann, wenn Pakete verloren gehen oder verworfen (engl. drop) werden. Der Empfänger-Computer teilt dem Absender nicht mit, wenn er ein Datenpaket erhält. Wenn Sie *UDP* gewählt haben, können Sie die gleichen Konfigurationsoptionen bearbeiten wie bei TCP.
- **TCP/UDP:** Hierbei handelt es sich um eine Kombination von TCP und UDP, die sich besonders für Anwendungsprotokolle eignet, die beide Unterprotokolle verwenden, z. B. DNS. Wenn Sie *TCP/UDP* gewählt haben, können Sie die gleichen Konfigurationsoptionen angeben wie bei TCP oder UDP.
- **ICMP/ICMPv6:** Das ICMP-Protokoll (*Internet Control Message Protocol*) wird hauptsächlich dazu verwendet, Fehlermeldungen zu versenden, die angeben, dass z. B. ein angeforderter Dienst nicht verfügbar ist oder dass ein Host oder Router nicht erreicht werden kann. Nachdem Sie *ICMP* oder *ICMPv6* gewählt haben, geben Sie den ICMP-Typ/-Code an. Beachten Sie, dass IPv4-Firewallregeln nicht für ICMPv6-Verkehr gelten und IPv6-Firewallregeln nicht für ICMP-Verkehr.
- **IP:** Das *Internet-Protokoll* (Internet Protocol, IP) ist ein Netzwerk- und Transportprotokoll für den Datenaustausch über das Internet. Nachdem Sie *IP* gewählt haben, geben Sie die Nummer desjenigen Protokolls an, das in IP eingebettet werden soll, z. B. `121` (steht für das SMP-Protokoll).
- **ESP:** Das ESP-Protokoll (*Encapsulating Security Payload*) ist Teil des IPSec-Tunnelprotokoll-Pakets, welches Verschlüsselungsdienste für Daten bietet, die über VPN-Tunnel gesendet werden. Nach der Auswahl von ESP oder AH geben Sie

den *Sicherheitsparameterindex* (SPI) an, der in Verbindung mit der IP-Adresse die Sicherheitsparameter identifiziert. Sie können entweder einen Wert zwischen 256 und 4.294.967.296 angeben, oder die Voreinstellung des Bereichs 256 bis 4.294.967.296 (Doppelpunkt als Trennzeichen) beibehalten, insbesondere wenn Sie automatischen Schlüsselaustausch für IPsec verwenden. Beachten Sie, dass die Zahlen 1–255 von der IANA (*Internet Assigned Numbers Authority*) reserviert sind.

- **AH:** Die *Authentifizierungskopfzeile* (Authentication Header, AH) ist Teil der IPsec-Tunnelprotokoll-Lösung und befindet sich zwischen der IP-Kopfzeile (header) und den Datagramm-Nutzdaten (payload), um die Integrität der Daten zu verwalten – jedoch nicht deren Geheimhaltung.
- **Gruppe:** Hierbei handelt es sich um eine Art Behälter, der eine Liste anderer Dienstdefinitionen enthält. Sie können ihn verwenden, um Dienstdefinitionen zusammenzufassen, damit Ihre Konfiguration übersichtlicher wird.Nachdem Sie *Gruppe* gewählt haben, erscheint das Feld *Mitglieder*, in das Sie Gruppenmitglieder, d. h. andere Dienstdefinitionen, hinzufügen können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Definition wird in der Liste *Dienstdefinitionen* angezeigt.

Um eine Definition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Hinweis – Der Typ der Definition kann im Nachhinein nicht mehr geändert werden. Wenn Sie den Typ einer Definition ändern wollen, müssen Sie die Dienstdefinition löschen und eine neue mit den gewünschten Einstellungen anlegen.

5.3 Zeitraumdefinitionen

Auf der Seite *Definitionen & Benutzer > Zeitraumdefinitionen* werden einzelne oder wiederkehrende Zeitfenster definiert, die dazu verwendet werden können, beispielsweise Firewallregeln oder Inhaltsfilterprofile auf bestimmte Zeiträume zu beschränken.

Tipp – Durch einen Klick auf das Infosymbol einer Zeitraumdefinition in der Liste *Zeitraumdefinitionen* werden Ihnen alle Konfigurationsoptionen angezeigt, in denen diese Zeitraumdefinition verwendet wird.

Um eine Zeitraumdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zeitraumdefinitionen* auf *Neue Zeitraumdefinition*.**
   Das Dialogfeld *Neue Zeitraumdefinition erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Zeitraumdefinition ein.

   Art: Wählen Sie den Typ des Zeitraums aus. Die folgenden Typen sind verfügbar:

   - **Wiederkehrendes Ereignis:** Diese Ereignisse kehren periodisch wieder. Sie können Startzeit, Endzeit und die Wochentage angeben, für die diese Zeitraumdefinition gelten soll. Falls der Zeitraum bis in den nächsten Tag reicht, bezieht sich der ausgewählte Wochentag auf den Startzeitpunkt. Ein Start- oder Enddatum kann für diesen Typ nicht ausgewählt werden.

   - **Einzelereignis:** Diese Ereignisse finden nur einmal statt. Sie können sowohl Startdatum und -zeit als auch Enddatum und -zeit auswählen.Da diese Definitionen keine wiederkehrenden Ereignisse sind, können Sie die Option *Wochentage* für diesen Typ nicht auswählen.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Zeitraumdefinition wird in der Liste *Zeitraumdefinitionen* angezeigt.

Um eine Zeitraumdefinition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

5.4 Benutzer & Gruppen

Über das Menü *Definitionen & Benutzer > Benutzer & Gruppen* können Sie Benutzer und Gruppen für den Zugriff auf den WebAdmin sowie den Fernzugriff, den Zugriff auf das Benutzerportal und die E-Mail-Nutzung erstellen.

5.4.1 Benutzer

Auf der Registerkarte *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer* können Sie Benutzerkonten zur UTM hinzufügen.In der Werkseinstellung besitzt Sophos UTM einen vorkonfigurierten Administrator namens *admin*.

Tipp – Durch einen Klick auf das Infosymbol einer Benutzerdefinition in der Liste *Benutzer* werden Ihnen alle Konfigurationsoptionen angezeigt, in denen diese Benutzerdefinition verwendet wird.

Wenn Sie eine E-Mail-Adresse im Dialogfeld *Neuer Benutzer* angeben, wird parallel zum Anlegen der Benutzerdefinition ein X.509-Zertifikat generiert. Dabei dient die E-Mail-Adresse als VPN-ID. Andernfalls, wenn keine E-Mail-Adresse angegeben ist, wird ein Zertifikat generiert, das den *Distinguished Name* (DN) des Benutzers als VPN-ID verwendet. Wenn sich ein Benutzer über eine Backend-Gruppe wie z. B. eDirectory authentifiziert, wird dadurch ein Zertifikat angelegt, selbst wenn keine E-Mail-Adresse in der entsprechenden Backend-Benutzerdefinition angegeben ist.

Da die VPN-ID jedes Zertifikats einzigartig sein muss, muss jede Benutzerdefinition eine unterschiedliche und einzigartige E-Mail-Adresse besitzen. Das Anlegen einer Benutzerdefinition mit einer bereits vorhandenen E-Mail-Adresse ist nicht möglich. Diese Zertifikate können für verschiedene Fernzugriff-Methoden verwendet werden, die von Sophos UTM unterstützt werden, mit Ausnahme von PPTP, L2TP über IPsec unter Verwendung von PSK und nativem IPsec unter Verwendung von RSA oder PSK.

Um ein Benutzerkonto hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Benutzer* auf *Neuer Benutzer*.**
   Das Dialogfeld *Neuen Benutzer erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Benutzername: Tragen Sie einen aussagekräftigen Namen für diesen Benutzer ein (z. B. Max Mustermann). Beachten Sie, dass ein Benutzername nur druckbare ASCII-Zeichen enthalten darf, wenn er für Fernzugriff über PPTP oder L2TP über IPsec genutzt werden soll[1].

[1] http://de.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

Realname: Tragen Sie den Realnamen des Benutzers ein (z. B. Max Mustermann).

E-Mail-Adresse: Tragen Sie die primäre E-Mail-Adresse des Benutzers ein.

Zusätzliche E-Mail-Adressen (optional): Geben Sie zusätzliche E-Mail-Adressen dieses Benutzers ein. Alle als Spam eingestuften E-Mails an diese Adressen werden in einem individuellen Quarantänebericht gesondert aufgeführt. Dieser Quarantänebericht wird an die primäre E-Mail-Adresse geschickt.

Authentifizierung: Wählen Sie die Authentifizierungsmethode. Die folgenden Methoden sind verfügbar:

- **Lokal:** Wählen Sie diese Methode, um den Benutzer lokal an der UTM zu authentifizieren.
- **Entfernt:** Der Benutzer authentifiziert sich über eine externe Authentifizierungsmethode, die von Sophos UTM unterstützt wird. Weitere Informationen finden Sie unter *Definitionen & Benutzer > Authentifizierungsdienste*.
- **Keine:** Wählen Sie diese Methode, um zu verhindern, dass der Benutzer sich authentifizieren kann. Dies ist beispielsweise nützlich, um einen Benutzer vorübergehend zu deaktivieren, ohne die Benutzerdefinition vollständig löschen zu müssen.

Kennwort: Tragen Sie das Kennwort für den Benutzer ein (ein zweites Mal zur Bestätigung). Diese Option ist nur verfügbar, wenn Sie als Authentifizierungsmethode *Lokal* gewählt haben. Beachten Sie, dass die einfache Benutzerauthentifizierung keine Umlaute unterstützt.Beachten Sie, dass ein Kennwort nur druckbare ASCII-Zeichen enthalten darf, wenn es für Fernzugriff über PPTP oder L2TP über IPsec genutzt werden soll[1].

Backend-Sync: Einige Grundeinstellungen, wie der echte Name und die E-Mail-Adresse des Benutzers werden automatisch durch Synchronisation mit dem externen Backend-Authentifizierungsserver aktualisiert (diese Option ist nur verfügbar, wenn Sie als Authentifizierungsmethode *Entfernt* gewählt haben). Beachten Sie, dass diese Option automatisch entsprechend der Option *Aktiviere Backend-Synchronisierung bei Anmeldung* auf der Registerkarte *Authentifizierungsdienste > Erweitert* gesetzt wird, falls der Benutzer für das Vorabholen ausgewählt ist.

[1] http://de.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

> **Hinweis –** Momentan können Daten nur mit Active-Directory- und eDirectory-Servern synchronisiert werden.

X.509-Zertifikat: Sobald die Benutzerdefinition angelegt wurde, können Sie diesem Benutzer ein X.509-Zertifikat zuweisen, wenn Sie die Benutzerdefinition bearbeiten. Standardmäßig handelt es sich dabei um jenes Zertifikat, das beim Anlegen der Benutzerdefinition erzeugt wurde. Sie können jedoch auch ein Zertifikat eines Drittanbieters zuweisen, das Sie auf der Registerkarte *Fernzugriff* > *Zertifikatverwaltung* > *Zertifikate* hochladen können.

Statische Fernzugriffs-IP verwenden (optional): Wählen Sie diese Option aus, wenn Sie einem Benutzer, der Fernzugriff verwendet, eine statische IP-Adresse anstelle einer dynamischen IP-Adresse aus einem IP-Adressenpool zuweisen möchten. Für IPsec-Benutzer hinter einem NAT-Router ist es beispielsweise zwingend erforderlich, eine statische IP-Adresse zu verwenden.

> **Hinweis –** Die statische IP-Adresszuweisung kann nur für den Fernzugriff via PPTP, L2TP und IPsec genutzt werden.Sie kann jedoch nicht für den Fernzugriff via SSL genutzt werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Benutzer können ihre eigene Whitelist und Blacklist mit E-Mail-Adressen erstellen und verwalten (siehe Kapitel Benutzerportal). Sie können diese Listen hier anzeigen und bei Bedarf ändern.
4. **Klicken Sie auf *Speichern*.**
   Das neue Benutzerkonto wird anschließend in der Liste *Benutzer* angezeigt.

Wenn Sie diesem Benutzer reguläre Administrationsrechte mit Zugriff auf die webbasierte Administrationsschnittstelle WebAdmin geben wollen, fügen Sie den Benutzer zur Gruppe *SuperAdmins* hinzu, die auf der Registerkarte *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Gruppen* konfiguriert wird.

> **Hinweis –** Wenn Sie ein Benutzerobjekt gelöscht haben und ein Benutzerkonto mit demselben Namen anlegen wollen, stellen Sie sicher, dass Sie auch das zugehörige Zertifikat auf

der Registerkarte *Fernzugriff* > *Zertifikatverwaltung* > *Zertifikate* gelöscht haben. Andernfalls erhalten Sie eine Fehlermeldung, dass ein Benutzerkonto mit diesem Namen bereits existiert.

Sie können Zertifikate für den Fernzugriff und/oder Konfigurationen von Benutzern herunterladen, für die eine Art des Fernzugriffs aktiviert wurde. Aktivieren Sie dazu das Auswahlkästchen vor den jeweiligen Benutzern und wählen Sie die gewünschte Option im Tabellenkopf aus der Auswahlliste *Aktionen* aus. Benutzer mit Fernzugriff können diese Dateien auch selbst herunterladen, sofern Sie Zugriff auf das Benutzerportal haben.

5.4.2 Gruppen

Auf der Seite *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Gruppen* können Sie Benutzergruppen zur UTM hinzufügen.In der Werkseinstellung ist in der Sophos UTM eine Benutzergruppe *SuperAdmins* vorhanden. Wenn Sie einem Benutzer administrative Rechte geben wollen, d. h. Zugriffsrechte auf den WebAdmin, fügen Sie ihn der Gruppe *SuperAdmins* hinzu; diese Gruppe sollte nicht gelöscht werden.

Tipp – Durch einen Klick auf eine Gruppendefinition in der Liste *Gruppen* werden Ihnen alle Konfigurationsoptionen angezeigt, in denen diese Gruppendefinition verwendet wird.

Um eine Benutzergruppe hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Gruppen* auf *Neue Gruppe*.**
   Das Dialogfeld *Neue Gruppe erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Gruppenname: Geben Sie einen aussagekräftigen Namen für diese Gruppe ein. Der Gruppenname muss nicht mit dem Gruppennamen Ihrer Backend-Gruppen übereinstimmen.

   Gruppentyp: Wählen Sie den Gruppentyp aus. Sie können zwischen einer Gruppe mit statischen Mitgliedern und zwei Gruppen mit dynamischer Mitgliedschaft wählen.

   - **Statische Mitglieder:** Wählen Sie die lokalen Benutzer aus, die Mitglied in dieser Gruppe werden sollen.

   - **IPsec-X509-DN-Maske:** Benutzer werden dynamisch zu einer IPsec-X509-DN-Gruppendefinition hinzugefügt, sobald sie sich erfolgreich über eine IPsec-

Verbindung am Gateway angemeldet haben und spezifische Parameter ihres Distinguished Name mit dem Wert im Feld *DN-Maske* übereinstimmen.

- **Backend-Mitgliedschaft:** Benutzer werden dynamisch zur einer Gruppendefinition hinzugefügt, wenn sie sich erfolgreich an einem der unterstützten Authentifizierungsdienste angemeldet haben.Um fortzufahren, wählen Sie die entsprechende Backend-Authentifizierungsmethode aus:
  - **Active Directory:** Eine Active-Directory-Benutzergruppe der UTM stellt die Gruppenmitgliedschaft für Mitglieder von Active-Directory-Server-Benutzergruppen bereit, die in einem Windows-Netzwerk konfiguriert sind. Weitere Informationen finden Sie unter *Definitionen & Benutzer > Authentifizierungsdienste > Server*.
  - **eDirectory:** Eine eDirectory-Benutzergruppe der UTM stellt die Gruppenmitgliedschaft für Mitglieder von eDirectory-Benutzergruppen bereit, die in einem eDirectory-Netzwerk konfiguriert sind. Weitere Informationen finden Sie unter *Definitionen & Benutzer > Authentifizierungsdienste > Server*.
  - **RADIUS:** Benutzer werden automatisch zu einer RADIUS-Backend-Gruppe hinzugefügt, wenn sie sich erfolgreich über die RADIUS-Authentifizierungsmethode authentifiziert haben.
  - **TACACS+:** Benutzer werden automatisch zu einer TACACS+-Backend-Gruppe hinzugefügt, wenn sie sich erfolgreich über die TACACS+-Authentifizierungsmethode authentifiziert haben.
  - **LDAP:** Benutzer werden automatisch zu einer LDAP-Backend-Gruppe hinzugefügt, wenn sie sich erfolgreich über die LDAP-Authentifizierungsmethode authentifiziert haben.

Auf Backend-Gruppenmitglieder beschränken (optional; nur mit den Backend-Gruppen *Active Directory* oder *eDirectory*): In Netzwerken mit einem X.500-Verzeichnisdienst kann die Mitgliedschaft auf bestimmte Gruppen auf Ihrem Backend-Server beschränkt werden, wenn Sie nicht alle Benutzer des gewählten Backend-Servers in diese Gruppendefinition aufnehmen wollen. Wenn Sie diese Option wählen, müssen die hier angegebenen Gruppen mit einem *Allgemeinen Namen* (Common Name) übereinstimmen, der auf Ihrem Backend-Server konfiguriert ist. Beachten Sie, dass Sie das `CN=`-Präfix weglassen können, wenn Sie diese Option für Active Directory aktivieren. Wenn Sie diese Option für ein eDirectory-Backend aktivieren, können Sie den eDirectory-Browser

verwenden, um bequem die eDirectory-Gruppen auszuwählen, die in diese Gruppendefinition aufgenommen werden sollen. Falls Sie den eDirectory-Browser nicht verwenden, stellen Sie jedoch sicher, dass das `CN=`-Präfix vorhanden ist, wenn Sie eDirectory-Container eingeben.

Ein LDAP-Attribut überprüfen (optional; nur mit Backend-Gruppe *LDAP*): In Netzwerken mit einem LDAP-Verzeichnisdienst kann die Mitgliedschaft auf bestimmte Gruppen in der Datenbank begrenzt werden, die ein bestimmtes LDAP-Attribut Ihres Backend-Servers aufweisen, wenn Sie nicht alle Benutzer eines gewählten LDAP-Backend-Servers in diese Gruppendefinition aufnehmen wollen. Dieses Attribut wird dann als LDAP-Filterkriterium verwendet.Beispiel: Sie könnten `groupMembership` als Attribut mit dem Wert `CN=Sales,O=Beispiel` angeben. Dadurch würden alle Benutzer aus der Vertriebsabteilung Ihrer Firma zur Gruppendefinition hinzugefügt werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Benutzergruppe wird anschließend in der Liste *Gruppen* angezeigt.

Um eine Gruppe zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

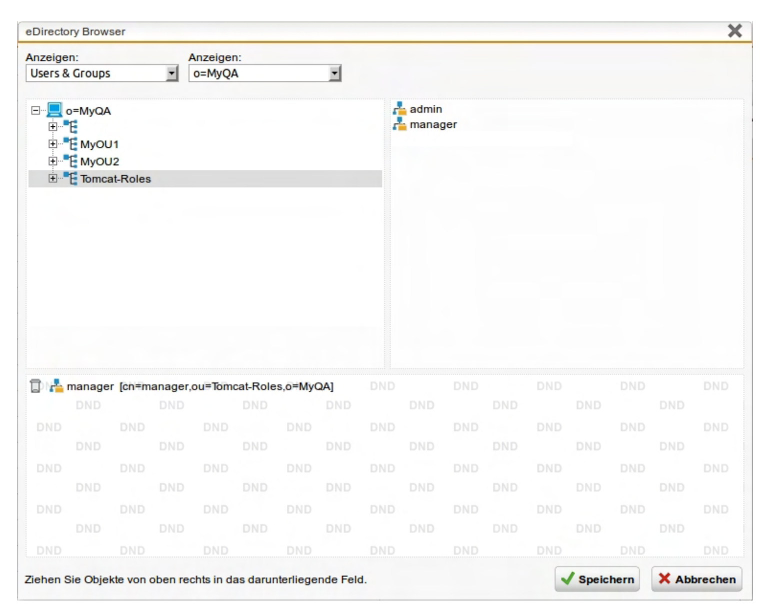


Bild 17 Gruppen: eDirectory-Browser von Sophos UTM

5.5 Client-Authentifizierung

Sophos stellt einen Authentifizierungsclient für Windows zur Verfügung, sodass sich die Benutzer direkt bei der UTM authentifizieren können. Dies ermöglicht eine benutzerbasierte Kontrolle über das Surfen im Internet sowie den Netzwerkverkehr, da z. B. auf Benutzernetzwerken oder Gruppennetzwerken basierende Firewallregeln erstellt werden können. Zudem werden, falls möglich, IP-Adressen, Hostnamen und ähnliche Elemente durch Benutzernamen ersetzt, sodass Berichtsdaten und Objekte besser verständlich sind.

Hinweis – Im WebAdmin werden Benutzernetzwerkobjekte, die über die Client-Authentifizierung authentifiziert sind, aus Leistungsgründen immer als nicht aufgelöst (unresolved) angezeigt.

Benutzer, die Client-Authentifizierung nutzen möchten oder sollen, müssen den Sophos Authentication Agent (SAA) auf Ihrem Client-PC oder Mac-OS-Computer installieren. Der SAA kann von dieser WebAdmin-Seite oder im Benutzerportal heruntergeladen werden. Beachten

Sie, dass der Download-Link im Benutzerportal nur für Benutzer verfügbar ist, die Teil der Benutzergruppe für die Client-Authentifizierungskonfiguration sind.

Um Client-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Client-Authentifizierung* die Client-Authentifizierung.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und der Abschnitt *Client-Authentifizierungsoptionen* kann nun bearbeitet werden.

2. **Wählen Sie die zugelassenen Netzwerke aus.**
   Wählen Sie die Netzwerke aus oder fügen Sie Netzwerke hinzu, die Client-Authentifizierung verwenden sollen.Beachten Sie, dass diese Netzwerke direkt mit der UTM verbunden sein müssen, da die Client-Authentifizierung andernfalls nicht funktioniert. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

3. **Wählen Sie die zugelassenen Benutzer und Gruppen aus.**
   Wählen Sie im Feld *Zugelassene Benutzer und Gruppen* einzelne Benutzer oder Gruppen aus oder fügen Sie neue Benutzer hinzu. Sie können auch eine bereits bestehende Authentifizierungsgruppe, z. B. eine Active-Directory-Benutzergruppe, auswählen. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

   Client-Authentifizierung ist nun für die ausgewählten Netzwerke verfügbar.

Client-Authentifizierungsprogramm

Wenn Client-Authentifizierung aktiviert ist, können Sie den Sophos Authentication Agent (SAA) hier herunterladen. Sie können den SAA manuell bereitstellen oder die Benutzer laden den Client direkt vom Benutzerportal herunter.

EXE herunterladen: Lädt das Client-Authentifizierungsprogramm einschließlich des CA-Zertifikats herunter, das der direkten Installation auf Client-PCs dient. Das ist die gleiche Datei, die auch im Benutzerportal heruntergeladen werden kann.

MSI herunterladen: Lädt das MSI-Paket für die Client-Authentifizierung herunter. Dieses Paket ist für die automatische Paket-Installation über Domain Controller (DC) gedacht und enthält kein CA-Zertifikat.

DMG herunterladen: Lädt das Disk-Image (Speicherabbild) für die Client-Authentifizierung auf Mac OS X herunter. Dieses Image dient der Installation auf Client-Computern mit dem Betriebssystem Mac OS X.

CA herunterladen: Lädt das CA-Zertifikat herunter, das zusätzlich zum MSI-Paket ausgerollt werden muss.

Der SAA kann als Authentifizierungsmethode für den Webfilter genutzt werden.Weitere Informationen hierzu finden Sie im Kapitel *Web Protection* > *Webfilter* > *Allgemein*.

5.6 Authentifizierungsdienste

Auf der Seite *Definitionen & Benutzer* > *Authentifizierungsdienste* können Datenbanken und Backend-Server externer Dienste zur Benutzerauthentifizierung wie Single Sign-On oder Einmaliges Kennwort verwaltet werden. Externe Benutzerauthentifizierung ermöglicht es Ihnen, Benutzerkonten gegen vorhandene Benutzerdatenbanken oder Verzeichnisdienste zu validieren, die sich auf anderen Servern in Ihrem Netzwerk befinden. Momentan werden folgende Authentifizierungsdienste unterstützt:

- Novell eDirectory
- Microsoft Active Directory
- RADIUS
- TACACS+
- LDAP

5.6.1 Allgemein

Auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsserver* > *Allgemeine Einstellungen* können Sie die grundlegenden Einstellungen für die Authentifizierung vornehmen. Die folgenden Optionen sind möglich:

Benutzer automatisch erstellen: Wenn diese Option ausgewählt ist, legt Sophos UTM automatisch ein Benutzerobjekt an, sobald sich ein unbekannter Benutzer einer konfigurierten Backend-Gruppe erfolgreich über einen der angebundenen Authentifizierungsdienste anmeldet, der von der Sophos UTM unterstützt wird. Beispiel: Wenn Sie eine RADIUS-Backend-Gruppe konfigurieren und diese Gruppe als Mitglied zu einer der Rollen hinzufügen, die auf der Registerkarte *Verwaltung* > *WebAdmin-Einstellungen* > *Zugriffskontrolle* definiert sind, erstellt

die Sophos UTM automatisch eine Benutzerdefinition für RADIUS-Benutzer, die sich erfolgreich am WebAdmin angemeldet haben.

- **Automatische Benutzererstellung für Komponenten:** Für bestimmte Funktionen kann eine automatische Benutzererstellung aktiviert oder deaktiviert werden. Die Benutzer werden dabei nur für die ausgewählten Funktionen angelegt. Diese Option ist nicht verfügbar – und automatische Benutzererstellung ist für alle Komponenten deaktiviert – wenn die Option *Benutzer automatisch erstellen* nicht ausgewählt ist.

  Hinweis – Diese Funktion ist mit Active Directory *Single Sign-On* (SSO) nicht möglich.

Diese Benutzerobjekte werden auch benötigt, um Zugang zum Benutzerportal der Sophos UTM zu gewähren. Darüber hinaus wird für alle automatisch erstellten Benutzerobjekte ein X.509-Zertifikat generiert. Beachten Sie jedoch, dass die automatische Benutzererstellung fehlschlägt, wenn es zu einem E-Mail-Adressenkonflikt kommt, da die zu erstellende Benutzerdefinition keine E-Mail-Adresse besitzen darf, die auf dem System bereits vorhanden ist. Alle E-Mail-Adressen müssen innerhalb des Systems eindeutig sein, da sie zur Identifizierung der X.509-Zertifikate dienen.

Wichtiger Hinweis – Authentifizierung (das Herausfinden, wer ein Benutzer ist) und Autorisierung (das Herausfinden, was ein Benutzer darf) für einen Benutzer, dessen Benutzerobjekt automatisch erstellt wurde, geschieht immer auf dem entfernten Backend-Server bzw. Verzeichnisdienst. Aus diesem Grund sind automatisch erzeugte Benutzerobjekte in der Sophos UTM nutzlos, wenn der entsprechende Backend-Server nicht erreichbar ist oder das Benutzerobjekt am entfernten Standort gelöscht wurde.

Beachten Sie auch, dass die Sophos UTM Benutzerauthentifizierungsdaten, die es von einem entfernten Authentifizierungsserver geholt hat, für 300 Sekunden zwischenspeichert. Ausgenommen hiervon ist Active Directory *Single Sign-On* (SSO). Deshalb werden sich Änderungen an den entfernten Benutzereinstellungen erst auswirken, wenn der Speicherzeitraum abgelaufen ist.

Authentifizierungs-Cache

Jedes Mal, wenn die Sophos UTM eine Benutzeranfrage von einem noch unbekannten Benutzer erreicht, z. B. `http`, und Authentifizierung erforderlich ist, schreibt die Sophos User Authentication (SUA) einen Eintrag in den Authentifizierungs-Cache. Mit der Zeit kann es in Umgebungen mit häufig wechselnden Benutzern sinnvoll sein, den Cache gelegentlich zu leeren. Eine Leerung kann auch angebracht sein, wenn Sie für alle Benutzer eine sofortige neue

Authentifizierung erzwingen wollen. Verwenden Sie die Schaltfläche *Auth.-Cache leeren*, um den Authentifizierungs-Cache zu leeren.
Eine Authentifizierung ist 300 Sekunden lang gültig. In dieser Zeit werden neue Authentifizierungsanfragen desselben Benutzers direkt im Cache abgefragt. Diese Methode entlastet Backend-Authentifizierungsdienste wie eDirectory.

Hinweis – Das Leeren des Caches hat keine Auswirkung auf augenblicklich entfernt angemeldete Benutzer.

Live-Protokoll

Live-Protokoll öffnen: Durch einen Klick auf die Schaltfläche wird das Protokoll der *Sophos User Authentication* (SUA) in einem neuen Fenster angezeigt.

5.6.2 Server

Auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsserver > Server* können Sie einen oder mehrere Authentifizierungsserver erstellen, u. a. eDirectory, Active Directory, LDAP, RADIUS und TACACS+.

5.6.2.1 eDirectory

Novell eDirectory ist ein X.500-kompatibler Verzeichnisdienst zur zentralen Verwaltung von Zugriffsrechten auf Ressourcen auf mehreren Servern und Hosts innerhalb eines bestimmten Netzwerks. eDirectory ist eine hierarchische, objektorientierte Datenbank, die alle Bestandteile einer Organisation in einer logischen Baumstruktur darstellt. Diese Bestandteile können Menschen, Server, Workstations, Anwendungen, Drucker, Dienste, Gruppen usw. sein.

Um eDirectory-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Auth-Server*.**
   Das Dialogfeld *Neuen Authentifizierungsserver anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Backend: Wählen Sie *eDirectory* als Backend-Verzeichnisdienst.

   Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

Server: Wählen Sie einen eDirectory-Server (oder fügen Sie einen hinzu). Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

SSL: Wählen Sie diese Option, um SSL-gesicherten Datentransfer zu aktivieren. Der *Port* ändert sich dann von `389` (LDAP) auf `636` (ldaps = LDAP over SSL).

Port: Wählen Sie den Port des eDirectory-Servers.Standardmäßig ist das Port `389`.

Bind-DN: Der *Distinguished Name* (DN) des Benutzers, mit dem dieser am Server angemeldet werden soll. Dieser Benutzer wird benötigt, wenn anonyme Anfragen an den eDirectory-Server nicht erlaubt sind. Beachten Sie, dass der Benutzer genügend Privilegien besitzen muss, um alle relevanten Informationen zur Benutzerdefinition vom eDirectory-Server erhalten zu können, damit er Benutzer authentifizieren kann.eDirectory-Benutzer, -Gruppen und -Container können mit dem vollständigen Distinguished Name in LDAP-Notation und Kommas als Trennzeichen angegeben werden (z. B. `CN=administrator,DC=intranet,DC=beispiel,DC=de`).

Kennwort: Geben Sie das Kennwort des Bind-Benutzers ein.

Servereinstellungen testen: Durch einen Klick auf die Schaltfläche *Test* wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, dass der Server eingeschaltet ist und Verbindungen annimmt.

BaseDN: Der Startpunkt, relativ gesehen zur Wurzel (engl. root) des LDAP-Baums, in dem die Benutzer eingefügt sind, die authentifiziert werden sollen. Beachten Sie, dass der BaseDN über den vollen Distinguished Name (FDN) in LDAP-Notation spezifiziert werden muss, wobei Kommata als Trennzeichen verwendet werden müssen (z. B. `O=Beispiel,OU=RnD`). Der BaseDN kann leer sein. In diesem Fall wird der BaseDN automatisch aus dem Verzeichnis abgerufen.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert und dass Benutzer erfolgreich authentifiziert werden können.

3. **Klicken Sie auf *Speichern*.**
   Der Server wird in der Liste *Server* angezeigt.

5.6.2.2 Active Directory

Microsoft Active Directory (AD) ist ein Verzeichnisdienst und eine zentrale Komponente der Windows 2000/2003 Server. Es speichert Informationen aus einem breiten Spektrum von Netzwerkressourcen, einschließlich Benutzer, Gruppen, Computer, Drucker, Anwendungen, Dienste und jeder Art von benutzerdefinierten Objekten. Als solches ist es ein Mittel, um diese Ressourcen zentral zu organisieren, zu verwalten und den Zugriff darauf zu kontrollieren.

Die Active-Directory-Authentifizierungsmethode ermöglicht es, die Sophos UTM an einer Windows-Domäne zu registrieren, wodurch ein Objekt für Sophos UTM auf dem primären *Domänencontroller* (DC) angelegt wird.UTMist dann in der Lage, Benutzer- und Gruppeninformationen von der Domäne abzufragen.

Hinweis – UTM unterstützt Active Directory 2003 und neuer.

Um Active-Directory-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Auth-Server*.**
   Das Dialogfeld *Neuen Authentifizierungsserver anlegen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Backend: Wählen Sie *Active Directory* als Backend-Verzeichnisdienst.

   Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

   Server: Wählen Sie einen Active-Directory-Server (oder fügen Sie einen hinzu). Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   SSL: Wählen Sie diese Option, um SSL-gesicherten Datentransfer zu aktivieren. Der *Port* ändert sich dann von `389` (LDAP) auf `636` (ldaps = LDAP over SSL).

   Port: Geben Sie den Port des Active-Directory-Servers ein. Standardmäßig ist das Port `389`.

Bind-DN: Der vollständige *Distinguished Name* (DN) des Benutzers, mit dem dieser am Server angemeldet werden soll, in LDAP-Notation. Dieser Benutzer wird benötigt, wenn anonyme Anfragen an den Active-Directory-Server nicht erlaubt sind. Beachten Sie, dass der Benutzer genügend Privilegien besitzen muss, um alle relevanten Informationen zur Benutzerdefinition vom Active-Directory-Server erhalten zu können, damit er Benutzer authentifizieren kann – das ist eine Voraussetzung, die meistens vom Administrator der Domäne erfüllt wird.

Jeder DN besteht aus einem oder mehreren *Relative Distinguished Names* (RDN). Ein RDN setzt sich aus Attributen des Active-Directory-Benutzerobjekts zusammen und umfasst seinen Benutzernamen, den Knoten des Objekts und den höchsten DN des Servers. Die Definition erfolgt in der LDAP-Notation. Als Trennzeichen wird das Komma verwendet.

- Der Benutzername muss der Name des Benutzers sein, der in der Lage ist, auf das Verzeichnis zuzugreifen und folgendermaßen spezifiziert ist: `CN`-Bezeichner (z. B. `CN=user`). Obwohl die Nutzung eines beliebten Kontos mit Domänenberechtigungen, wie z. B. „admin“, möglich ist, wird als bessere Methode dringend empfohlen, einen Benutzer zu wählen, der keine Administrationsrechte besitzt, da es völlig ausreichend für diesen Benutzer ist, Leserechte auf alle Objekte des angegebenen BaseDN zu besitzen.
- Die Information über den Knoten, an dem sich das Benutzerobjekt befindet, muss alle Unterknoten zwischen dem Wurzelknoten und dem Benutzerobjekt umfassen und besteht gewöhnlich aus Komponenten wie sogenannten *Organisationseinheiten* (engl. organizational units) und dem *allgemeinen Namen* (CN, engl. common name). Organisationseinheiten (dargestellt durch ein Verzeichnis-/Buchsymbol in der Microsoft Management-Konsole) werden durch den `OU`-Bezeichner spezifiziert. Beachten Sie, dass die Reihenfolge der Knoten vom untersten zum obersten verläuft, d. h., dass spezifischere Elemente zuerst angegeben werden (z. B. `OU=Management_US,OU=Management`). Andererseits werden den Standardcontainer von Active Directory (dargestellt durch ein einfaches Verzeichnis-Symbol) wie z. B. der vordefinierte *Benutzer*-Knoten durch den `CN`-Bezeichner spezifiziert (z. B. `CN=Users`).
- Der oberste DN des Servers kann aus mehreren Domänenkomponenten (engl. domain component) bestehen, wobei jede durch den `DC`-Bezeichner spezifiziert wird. Beachten Sie, dass die Domänenkomponenten in der gleichen Reihenfolge angegeben werden wie der Domänenname. Beispiel: Wenn der Domänenname `beispiel.de` ist, dann ist der DN-Teil `DC=beispiel,DC=de`.

Ein Beispiel für einen Bind-Benutzer-DN, wenn der Benutzername `administrator` ist und sich das Benutzerobjekt im Container `Users` befindet in einer Domäne namens `beispiel.de`: `CN=administrator,CN=Users,DC=beispiel,DC=de`

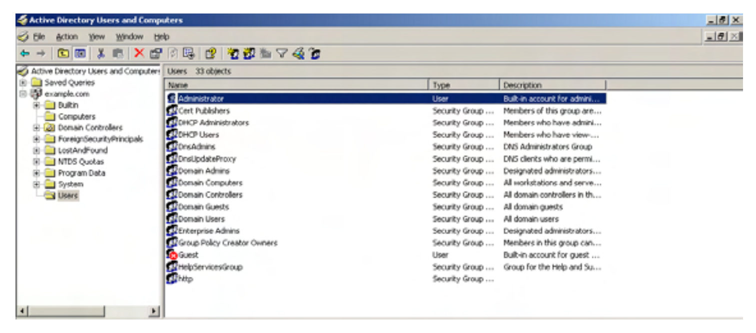


Bild 18 Authentifizierung: Microsoft Management-Konsole

Nehmen wir nun an, Sie haben eine Organisationseinheit namens *Management* mit dem Unterknoten *Management_US* angelegt und verschieben das Benutzerobjekt „Administrator“ dorthin, dann ändert sich der DN wie folgt:
`CN=administrator,OU=Management_US,OU=Management,DC=beispiel,DC=de`

Kennwort: Geben Sie das Kennwort des Bind-Benutzers ein.

Servereinstellungen testen: Durch einen Klick auf die Schaltfläche *Test* wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, dass der Server eingeschaltet ist und Verbindungen annimmt.

BaseDN: Der Startpunkt, relativ gesehen zur Wurzel (engl. root) des LDAP-Baums, in dem die Benutzer eingefügt sind, die authentifiziert werden sollen. Beachten Sie, dass der BaseDN über den vollen Distinguished Name (FDN) in LDAP-Notation spezifiziert werden muss, wobei Kommata als Trennzeichen verwendet werden müssen (z. B. `O=Beispiel,OU=RnD`). Der BaseDN kann leer sein. In diesem Fall wird der BaseDN automatisch aus dem Verzeichnis abgerufen.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert und dass Benutzer erfolgreich authentifiziert werden können.

3. **Klicken Sie auf *Speichern*.**
   Der Server wird in der Liste *Server* angezeigt.

5.6.2.3 LDAP

LDAP steht für *Lightweight Directory Access Protocol* und ist ein Netzwerkprotokoll, um Verzeichnisdienste, die auf dem X.500-Standard basieren, zu modifizieren und Anfragen zu senden. Sophos UTMverwendet das LDAP-Protokoll, um Benutzer für einige seiner Dienste zu authentifizieren, indem mithilfe von Attributen oder Gruppenzugehörigkeiten auf dem LDAP-Server festgestellt wird, ob Zugriff auf einen bestimmten Dienst gewährt wird oder nicht.

Um LDAP-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Auth-Server*.**
   Das Dialogfeld *Neuen Authentifizierungsserver anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Backend: Wählen Sie *LDAP* als Backend-Verzeichnisdienst.

   Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

   Server: Wählen Sie einen LDAP-Server (oder fügen Sie einen hinzu). Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   SSL: Wählen Sie diese Option, um SSL-gesicherten Datentransfer zu aktivieren. Der *Port* ändert sich dann von `389` (LDAP) auf `636` (ldaps = LDAP over SSL).

   Port: Wählen Sie den Port des LDAP-Servers.Standardmäßig ist das Port `389`.

   Bind-DN: Der *Distinguished Name* (DN) des Benutzers, mit dem dieser am Server angemeldet werden soll. Dieser Benutzer ist zwingend. Aus Sicherheitsgründen werden anonyme Anfragen an den LDAP-Server nicht unterstützt. Beachten Sie, dass der Benutzer genügend Privilegien besitzen muss, um alle relevanten Informationen zur

Benutzerdefinition vom LDAP-Server erhalten zu können, damit er Benutzer authentifizieren kann.LDAP-Benutzer, -Gruppen und -Container können mit dem vollständigen Distinguished Name in LDAP-Notation und Kommas als Trennzeichen angegeben werden (z. B. `CN=administrator,DC=intranet,DC=beispiel,DC=de`).

Kennwort: Geben Sie das Kennwort des Bind-Benutzers ein.

Servereinstellungen testen: Durch einen Klick auf die Schaltfläche *Test* wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, dass der Server eingeschaltet ist und Verbindungen annimmt.

Benutzerattribut: Wählen Sie das Benutzerattribut, das als Filter für die Suche im LDAP-Verzeichnis verwendet werden soll. Das Benutzerattribut enthält den eigentlichen Anmeldenamen, nach dem jeder Benutzer von z. B. Fernzugriffsdiensten gefragt wird. Folgende Benutzerattribute sind möglich:

- CN (allgemeiner Name, engl. common name)
- SN (Nachname)
- UID (Benutzer-ID)

Falls Benutzernamen in Ihrem LDAP-Verzeichnis nicht in Form dieser Attribute gespeichert werden, wählen Sie *<<Angepasst>>* aus der Liste aus und geben Sie Ihr benutzerdefiniertes Attribut im Feld *Angepasst* an. Beachten Sie, dass dieses Attribut in Ihrem LDAP-Verzeichnis konfiguriert sein muss.

BaseDN: Der Startpunkt, relativ gesehen zur Wurzel (engl. root) des LDAP-Baums, in dem die Benutzer eingefügt sind, die authentifiziert werden sollen. Beachten Sie, dass der BaseDN über den vollen Distinguished Name (FDN) in LDAP-Notation spezifiziert werden muss, wobei Kommata als Trennzeichen verwendet werden müssen (z. B. `O=Beispiel,OU=RnD`). Der BaseDN kann leer sein. In diesem Fall wird der BaseDN automatisch aus dem Verzeichnis abgerufen.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Ser-

vereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert und dass Benutzer erfolgreich authentifiziert werden können.

3. **Klicken Sie auf *Speichern*.**
   Der Server wird in der Liste *Server* angezeigt.

5.6.2.4 RADIUS

RADIUS steht für *Remote Authentication Dial In User Service* und ist ein weit verbreitetes Protokoll, mit dem Netzwerkgeräte, wie z. B. Router, Informationen für die Benutzerauthentifizierung von einem zentralen Server abfragen können. Neben den reinen Benutzerinformationen für die Authentifizierung kann RADIUS auch technische Informationen verwalten, die von Netzwerkgeräten genutzt werden. Dazu gehören z. B. verwendete Protokolle, IP-Adressen, Routeninformationen etc. Zusammen bilden sie ein Benutzerprofil, das in einer Datei oder Datenbank auf dem RADIUS-Server gespeichert wird.

Das RADIUS-Protokoll ist sehr flexibel und es gibt Server für die meisten Betriebssysteme. Die RADIUS-Implementierung auf der UTM ermöglicht es Ihnen, Zugriffsrechte basierend auf Proxys und Benutzern zu konfigurieren. Um die RADIUS-Authentifizierung verwenden zu können, benötigen Sie einen laufenden RADIUS-Server im Netzwerk. Kennwörter werden mit dem RADIUS-Schlüssel verschlüsselt, der Benutzername wird hingegen als Klartext übertragen.

Um RADIUS-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Auth-Server*.**
   Das Dialogfeld *Neuen Authentifizierungsserver anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Backend: Wählen Sie *RADIUS* als Backend-Verzeichnisdienst.

   Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

   Server: Wählen Sie einen RADIUS-Server (oder fügen Sie einen hinzu). Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Port: Wählen Sie den Port des RADIUS-Servers. Standardmäßig ist das Port `1812`.

Vereinbarter Schlüssel: Dieser vereinbarte Schlüssel (engl. Shared Secret) ist eine Zeichenfolge, die als Kennwort zwischen dem RADIUS-Client und dem RADIUS-Server dient. Geben Sie den vereinbarten Schlüssel ein.

Servereinstellungen testen: Durch einen Klick auf die Schaltfläche *Test* wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, dass der Server eingeschaltet ist und Verbindungen annimmt.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

NAS-Kennung: Wählen Sie die entsprechende NAS-Kennung aus der Liste. Weitere Informationen entnehmen Sie bitte dem untenstehenden Hinweis und der Tabelle.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert und dass Benutzer erfolgreich authentifiziert werden können.

3. **Klicken Sie auf *Speichern*.**
   Der Server wird in der Liste *Server* angezeigt.

Hinweis –Jeder Benutzerauthentifizierungsdienst von Sophos UTM (z. B. PPTP oder L2TP), der Anfragen an den RADIUS-Server stellt, sendet eine andere Kennung (NAS-Kennung, engl. NAS identifier) an den RADIUS-Server.Beispiel: Der PPTP-Dienst sendet die NAS-Kennung `pptp` an den RADIUS-Server, wenn er versucht, einen Benutzer zu authentifizieren. Dadurch können die verschiedenen Dienste auf dem RADIUS-Server auseinandergehalten werden. Das kommt den Autorisierungszwecken zugute, d. h. der Zugriffsgenehmigung für den Benutzer auf verschiedene Dienste. Unten finden Sie eine Liste der Benutzerauthentifizierungsdienste und ihrer NAS-Kennung.

Benutzerauthentifizierungsdienst	NAS-Kennung
SSL-VPN	`ssl`
PPTP	`pptp`

Benutzerauthentifizierungsdienst	NAS-Kennung
IPsec	`ipsec`
L2TP über IPsec	`l2tp`
SMTP-Proxy	`smtp`
Benutzerportal	`portal`
WebAdmin	`webadmin`
SOCKS-Proxy	`socks`
Webfilter	`http`
Authentifizierungsclient	`Agent`
Wireless Access Points	Die NAS-Kennung ist der Name des WLAN-Netzwerks.

Tabelle 1: RADIUS NAS-Kennungen

5.6.2.5 TACACS+

TACACS+ steht für *Terminal Access Controller Access Control System* und ist ein proprietäres Protokoll von Cisco Systems Inc., das detaillierte Netzwerkverkehrsinformationen liefert und administrative Kontrolle über Authentifizierungs- und Autorisierungsprozesse ermöglicht. Während RADIUS Authentifizierung und Autorisierung in einem Benutzerprofil kombiniert, trennt TACACS+ diese Vorgänge. Ein weiterer Unterschied ist, dass TACACS+ das TCP-Protokoll verwendet (Port `49`), wohingegen RADIUS das UDP-Protokoll verwendet.

Um TACACS+-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Auth-Server*.**
   Das Dialogfeld *Neuen Authentifizierungsserver anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Backend: Wählen Sie *TACACS+* als Backend-Verzeichnisdienst.

   Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher,

dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

Server: Wählen Sie einen TACACS+-Server (oder fügen Sie einen hinzu). Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Port: Geben Sie den Port des TACACS+-Servers ein. Standardmäßig ist das Port `49`.

Schlüssel: Geben Sie den Schlüssel für die Authentifizierung und die Verschlüsselung der gesamten TACACS+-Kommunikation zwischen Sophos UTM und dem TACACS+-Server ein. Der hier eingegebene Wert des Schlüssels muss mit demjenigen auf dem TACACS+-Server übereinstimmen. Geben Sie den Schlüssel ein (ein zweites Mal zur Bestätigung).

Servereinstellungen testen: Durch einen Klick auf die Schaltfläche *Test* wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, dass der Server eingeschaltet ist und Verbindungen annimmt.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert und dass Benutzer erfolgreich authentifiziert werden können.

3. **Klicken Sie auf *Speichern*.**
   Der Server wird in der Liste *Server* angezeigt.

5.6.3 Single Sign-On

Auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste > Single Sign-On* können Sie die Single-Sign-On-Funktionalität für Active Directory und/oder eDirectory konfigurieren.

Active Directory Single Sign-On (SSO)

Beachten Sie, dass die Active-Directory-SSO-Einrichtung augenblicklich nur mit dem Webfilter verwendet wird, um Single Sign-On für Browser bereitzustellen, die NTLMv2 oder Kerberos-

Authentifizierung unterstützen.

Um die Single-Sign-On-Funktionalität zu aktivieren, muss UTM der Active-Directory-Domäne beitreten. Damit dieser Domänenbeitritt funktioniert, müssen die folgenden Voraussetzungen erfüllt sein:

- Die Zeitzone auf dem Gateway und auf dem Domänencontroller (DC) müssen gleich sein.
- Der Zeitunterschied der Uhren auf dem Gateway und dem DC darf NICHT mehr als fünf Minuten betragen.
- Der UTM-Hostname muss im AD-DNS-System vorhanden sein.
- UTM muss das AD-DNS zur Weiterleitung (engl. forwarder) verwenden oder sie muss eine DNS-Anfrageroute zur AD-Domäne besitzen, die auf den AD-DNS-Server zeigt.

Um Active Directory SSO zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Legen Sie einen Active-Directory-Server auf der Registerkarte *Server* an.**
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Domäne: Name der Domäne (z. B. `intranet.meinefirma.de`). UTM sucht alle DCs, die über DNS erreichbar sind.

   Admin-Benutzername: Tragen Sie den Benutzernamen ein, der auch die Rechte für die Anbindung von Computern an diese Domäne besitzt (in der Regel ist dies der „Administrator").

   Kennwort: Das Kennwort für den Admin-Benutzer.
3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Hinweis zur Unterstützung der Kerberos-Authentifizierung: Damit die opportunistische SSO-Kerberos-Unterstützung funktioniert, MÜSSEN die Clients den FQDN-Hostnamen von UTM in ihren Proxyeinstellungen verwenden. Wenn sie die IP-Adresse verwenden, schlägt der Vorgang fehl. Der NTLMv2-Modus ist von dieser Voraussetzung nicht betroffen und wird automatisch genutzt, wenn diese Voraussetzung nicht erfüllt ist oder wenn der Browser eine Kerberos-Authentifizierung nicht unterstützt.

eDirectory Single Sign-On (SSO)

Hier können Sie SSO für eDirectory konfigurieren. Wenn Sie *eDirectory SSO* als Authentifizierungsmethode unter *Web Protection* > *Webfilter* eingerichtet haben, wird der hier

gewählte eDirectory-Server verwendet.

Um eDirectory SSO zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Legen Sie auf der Registerkarte *Server* einen eDirectory-Server an.**
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Server: Wählen Sie einen eDirectory-Server aus, für den Sie SSO aktivieren möchten.

   Sync-Interval: Die Zeit (in Sekunden) zwischen zwei Synchronisierungsereignissen zwischen UTM und eDirectory-Server.
3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

5.6.4 Einmaliges Kennwort (OTP)

Auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste > Einmaliges Kennwort* können Sie den Dienst für einmalige Kennwörter (OTP) konfigurieren und die Token der Benutzer einmaliger Kennwörter überwachen oder bearbeiten. Einmalige Kennwörter sind eine Methode zur Verbesserung der Sicherheit für kennwortbasierte Authentifizierung. Das benutzerspezifische Kennwort, das manchmal zu schwach ist, wird durch ein einmaliges Kennwort ergänzt, das für nur eine Anmeldung gültig ist. Selbst wenn ein Angreifer in den Besitz des Kennworts gelangt, kann er sich deshalb nicht damit anmelden.

Einmalige Kennwörter ändern sich im Allgemeinen ständig und in regelmäßigen Abständen. Sie werden automatisch durch einen bestimmten Algorithmus berechnet. Bald nachdem ein neues Kennwort berechnet wird, läuft das alte Kennwort automatisch ab. Um einmalige Kennwörter zu generieren, benötigt der Benutzer entweder ein Mobilgerät mit entsprechender Software oder spezielle Hardware oder ein Sicherheitstoken. Hardware-Token können von Beginn an verwendet werden. Der Endbenutzer muss auf dem Mobilgerät Google Authenticator oder eine ähnliche Software installieren und die Konfiguration implementieren, die im Benutzerportal als QR-Code, auf der Startseite oder auf der Seite *OTP-Token* verfügbar ist (siehe Seite *Benutzerportal*). Danach kann das Gerät einmalige Kennwörter in Token-spezifischen Intervallen generieren. Datum und Uhrzeit müssen auf dem Mobilgerät korrekt eingestellt sein, da der Zeitstempel bei der Generierung einmaliger Kennwörter verwendet wird.

> **Hinweis –** Um eine Authentifizierung für die Komponenten, für die ein einmaliges Kennwort erforderlich ist, durchzuführen, muss der Benutzer sein benutzerspezifisches UTM-Kennwort und direkt im Anschluss das einmalige Kennwort eingeben.

Der Administrator kann ebenfalls einmalige Kennwörter manuell generieren. Diese werden dann als Passcodes bezeichnet. In diesem Fall müssen Sie sicherstellen, dass diese zeitlich unbegrenzten einmaligen Kennwörter sicher zum Benutzer übertragen werden. Dieser Vorgang sollte jedoch nur eine Übergangslösung sein, beispielsweise, wenn ein Benutzer vorübergehend keinen Zugriff auf das Gerät hat, mit dem er Kennwörter generiert.

Hinweis – Sobald ein OTP-Token erstellt wurde wird rechts in der Tabelle ein Info-Symbol angezeigt. Sie können den QR-Code und dessen Details ansehen, indem Sie auf das Info-Symbol klicken.

Aktivierung und Konfiguration des Dienstes für einmalige Kennwörter

Zur Konfiguration des Dienstes für einmalige Kennwörter sind folgende Schritte erforderlich:

1. **Nehmen Sie im Bereich *OTP-Einstellungen* die folgenden Einstellungen vor:**
   Alle Benutzer müssen einmalige Kennwörter (OTP) verwenden: Standardmäßig ist diese Option aktiviert und alle Benutzer müssen einmalige Kennwörter verwenden. Wenn nur bestimmte Benutzer einmalige Kennwörter verwenden sollen, deaktivieren Sie die Option und wählen Sie Benutzer oder Gruppen aus oder fügen Sie sie im Feld hinzu.

   OTP-Token automatisch für Benutzer erstellen: Wenn diese Option ausgewählt ist, wird autorisierten Benutzern ein QR-Code zur Softwarekonfiguration auf dem Mobilgerät angezeigt, wenn sie sich das nächste Mal im Benutzerportal anmelden. Damit dies funktioniert, stellen Sie sicher, dass die Benutzer Zugriff auf das Benutzerportal haben (siehe Seiten *Verwaltung > Benutzerportal*). Wenn sich ein Benutzer im Benutzerportal anmeldet, wird das entsprechende Token in der Liste *OTP-Token* angezeigt. Es empfiehlt sich, diese Funktion zu aktivieren, wenn Sie Soft-Token auf Mobilgeräten verwenden. Wenn die Benutzer nur Hardware-Token verwenden, sollten Sie stattdessen die Option deaktivieren und die Token hinzufügen oder importieren, bevor Sie die OTP-Funktion aktivieren.

   OTP für Komponenten aktivieren: Hier wählen Sie die UTM-Komponenten aus, auf die die ausgewählten Benutzer mit einmaligen Kennwörtern zugreifen sollen. Wenn Sie die Option *OTP-Token automatisch für Benutzer erstellen*aktivieren, muss aus Sicherheitsgründen das Benutzerportal aktiviert sein: Da das Benutzerportal Zugriff auf die OTP-Token gewährt, sollte es selbst über mindestens den gleichen Schutz verfügen.

Um OTP für sicheren Shell-Zugriff zu aktivieren, müssen Sie für die entsprechenden Token zusätzlich die Verwendung für Shell-Zugriff aktivieren (siehe Manuelles Hinzufügen oder Bearbeiten von OTP-Token). Die entsprechenden Benutzer müssen sich dann mit dem zugehörigen Kennwort, an das das einmalige Kennwort angehängt wird, als *loginuser* anmelden.

Achtung – Stellen Sie insbesondere dann, wenn Sie den WebAdmin oder Shell-Zugriff zur Verwendung mit OTP auswählen, sicher, dass die ausgewählten Benutzer Zugriff auf die Token für einmalige Kennwörter haben. Andernfalls ist es möglich, dass Sie sie permanent abmelden.

Standard-Token-Zeitschritt: Um die Generierung einmaliger Kennwörter auf dem Mobilgerät und in der UTM zu synchronisieren, müssen die beiden Zeitschritte übereinstimmen. Einige Hardware-Token arbeiten mit einem Zeitschritt von 60 Sekunden. Google Authenticator nutzt beispielsweise einen Zeitschritt von 30 Sekunden, der hier dem Standardwert entspricht. Wenn die Zeitschritte nicht übereinstimmen, schlägt die Authentifizierung fehl. Der hier eingegebene Wert wird automatisch für jedes neue OTP-Token verwendet.

2. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

3. **Wenn Sie Hardware-Token verwenden, importieren Sie sie oder fügen Sie sie im Bereich *OTP-Token* hinzu.**
   Verwenden Sie die Daten vom Hardware-Token-Anbieter, um mithilfe von Semikolons eine UTF-8-codierte CSV-Datei zu generieren. Die Datei muss drei Spalten mit folgenden Inhalten enthalten: Schlüssel, Zeitschritt und Kommentar. Der Schlüssel, eine eindeutige, gerätespezifische Zeichenfolge, ist obligatorisch und sollte im Hexadezimalformat mit einer Länge von 128 bit vorliegen. Die anderen Spalten können leer sein.Wenn kein Zeitschritt angegeben wird, wird der Zeitschritt für das Standard-Token, der im Bereich *OTP-Einstellungen* festgelegt wird, verwendet.

   Klicken Sie rechts oberhalb der Liste auf das Importsymbol.Fügen Sie dann die Daten im CSV-Format in das Textfeld ein und klicken Sie auf *Speichern*.

   Nach dem Import können Sie die Einträge mithilfe des Bearbeitensymbols ändern.Außerdem können Sie immer einzelne Einträge hinzufügen, indem Sie auf das Plussymbol klicken (siehe Manuelles Hinzufügen oder Bearbeiten von OTP-Token).

4. **Aktivieren Sie den Dienst für einmalige Kennwörter.**
   Klicken Sie auf den Schieberegler oben auf der Seite.Der Schieberegler wird grün.

Wenn *OTP-Token automatisch für Benutzer erstellen* aktiviert ist, erstellt die UTM den OTP-Token-Eintrag automatisch, sofern er nicht vorab generiert wurde, wenn sich ein Benutzer, für den die Authentifizierung mit einem einmaligen Kennwort konfiguriert ist, erstmals im Benutzerportal anmeldet. Außerdem ist das Zurücksetzensymbol des Eintrags aktiviert.

Mithilfe des Schiebereglers eines Eintrags können sie diesen deaktivieren, zum Beispiel, wenn der Benutzer sein Hardware-Token verloren hat. Mit dem entsprechenden Symbol können Sie einen Eintrag löschen, beispielsweise, wenn ein Hardware-Token beschädigt ist. Achten Sie darauf, dass, wenn die Option *OTP-Token automatisch für Benutzer erstellen* aktiviert ist, der Benutzer in beiden Fällen eine erneute Authentifizierung durchführen kann, da er Zugriff auf den Token-Schlüssel hat.In der Liste *OTP-Token* wird ein neuer Eintrag angezeigt.

Mit dem Zurücksetzensymbol können Sie ein Token auf den Status „nie verwendet“ setzen, d. h., dem Benutzer wird der QR-Code erneut angezeigt, wenn er sich im Benutzerportal anmeldet.

Rechts oberhalb der Liste *OTP-Token* befinden sich ein Suchfeld und Navigationssymbole, mit denen Sie in der Liste navigieren und ihre Einträge filtern können.

Manuelles Hinzufügen oder Bearbeiten von OTP-Token

Sie können OTP-Token hinzufügen oder bearbeiten.

Tipp – Normalerweise fügen Sie keine einzelnen OTP-Token hinzu, sondern importieren sie entweder – wenn es sich um Hardware-Token handelt – oder generieren sie automatisch auf einem Mobilgerät mit der Option *OTP-Token automatisch für Benutzer erstellen*.

1. **Öffnen Sie das Dialogfenster, um das OTP-Token hinzuzufügen oder zu bearbeiten.**
   Um ein OTP-Token hinzuzufügen, klicken Sie rechts oberhalb der Liste *OTP-Token* auf das grüne Plussymbol.

   Um ein OTP-Token zu bearbeiten, klicken Sie auf das Bearbeitensymbol vor dem entsprechenden Eintrag in der Liste *OTP-Token*.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Benutzer: Wählen Sie den Benutzer, dem das Token zugewiesen werden soll, aus oder fügen Sie ihn hinzu.

   Schlüssel: Dies ist der vereinbarte Schlüssel des Hardware-Tokens oder Soft-Tokens des Benutzers. Ein Hardware-Token verfügt über einen unveränderlichen Schlüssel, der vom Hardwarehersteller festgelegt wird.Das Soft-Token wird nach dem Zufallsprinzip von der UTM generiert, wenn *OTP-Token automatisch für Benutzer erstellen* aktiviert ist. Der Schlüssel sollte im Hexadezimalformat vorliegen und 128 bit lang sein.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.Dieser Text wird mit dem QR-Code im Benutzerportal angezeigt. Wenn Sie verschiedene Token für eine Person festlegen, z. B. ein Hardware-Token und ein Soft-Token für das Mobiltelefon, ist es sinnvoll, hier eine Erläuterung anzugeben, da dem Benutzer alle QR-Codes nebeneinander angezeigt werden.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Benutzerdefinierten Token-Zeitschritt verwenden: Wenn Sie einen anderen Zeitschritt als den im Bereich *OTP-Einstellungen* festgelegten Standardzeitschritt für Token benötigen, aktivieren Sie diese Option und geben Sie den Wert ein. Der hier festgelegte Zeitschritt muss mit dem Zeitschritt auf dem Gerät, das der Benutzer zur Kennwortgenerierung verwendet, übereinstimmen. Ansonsten schlägt die Authentifizierung fehl.

   Token-Informationen im Benutzerportal verbergen: Wenn diese Option ausgewählt ist, wird das Token nicht im Benutzerportal angezeigt. Dies ist unter Umständen für Hardware-Token sinnvoll, für die keine Konfiguration erforderlich ist, oder wenn die Soft-Token beispielsweise nicht vom Endbenutzer konfiguriert werden sollen, sondern zentral vom Administrator.

   Token kann für Shell-Zugriff verwendet werden: Wenn diese Option ausgewählt ist, kann das Token für den Zugriff auf die UTM über die Kommandozeile verwendet werden. Damit dies funktioniert, muss Shell-Zugriff im Bereich *OTP-Einstellungen* aktiviert sein und Shell-Zugriff mit Kennwortauthentifizierung muss allgemein für die UTM aktiviert sein (siehe *Verwaltung* > *Systemeinstellungen* > *Shell-Zugriff*). OTP-Token mit Berechtigung für Shell-Zugriff weisen oben rechts ein Kommando-Shell-Symbol auf.Für Shell-Zugriff mit einem einmaligen Kennwort muss sich der Benutzer dann mit dem zugehörigen Kennwort, an das das einmalige Kennwort angehängt wird, als *loginuser* anmelden.

Zusätzliche Codes (nur bei Bearbeitung eines OTP-Tokens): Sie können einmalige Kennwörter für Token manuell hinzufügen. Klicken Sie entweder auf das grüne Plussymbol, um jeweils ein einmaliges Kennwort einzugeben, oder verwenden Sie die Schaltfläche *Generieren*, um zehn einmalige Kennwörter auf einmal zu generieren. Sie können die einmaligen Kennwörter auch mithilfe des Aktionssymbols importieren oder exportieren. Diese einmaligen Kennwörter sind zeitlich unbegrenzt. Ein einmaliges Kennwort wird automatisch gelöscht, wenn sich der Benutzer damit anmeldet. OTP-Token mit zusätzlichen einmaligen Kennwörtern weisen rechts ein Plussymbol auf. Wenn Sie mit dem Mauszeiger darüber fahren, wird die Liste der einmaligen Kennwörter angezeigt.

4. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

5.6.5 Erweitert

Erraten von Kennwörtern blockieren

Diese Funktion kann verwendet werden, um das Erraten von Kennwörtern zu verhindern.Nach einer bestimmten Anzahl von fehlgeschlagenen Versuchen (standardmäßig drei) wird der Zugriff von dieser IP-Adresse auf eine der Komponenten für eine bestimmte Zeit (standardmäßig 600 Sekunden) verweigert.

Pakete von blockierten Hosts verwerfen: Wenn diese Option aktiv ist, werden alle Pakete, die von blockierten Hosts kommen, für die festgelegte Zeit verworfen.Diese Option dient dazu, DoS-Attacken zu verhindern.

Komponenten: Die Überprüfung wird für die ausgewählten Komponenten durchgeführt.

Netzwerke nie blockieren: Die in diesem -Feld aufgelisteten Netzwerke werden von dieser Überprüfung ausgenommen.

Lokale Authentifizierungskennwörter

Mit dieser Option können Sie festlegen, dass Administratoren oder lokal registrierte Benutzer mit administrativen Rechten sichere Kennwörter verwenden müssen. Die Kennwortkomplexität kann so konfiguriert werden, dass sie den folgenden Sicherheitsanforderungen entspricht:

- Mindestlänge des Kennworts (acht Zeichen ist voreingestellt)
- mindestens ein kleingeschriebener Buchstabe
- mindestens ein großgeschriebener Buchstabe

- mindestens eine Zahl
- mindestens ein nicht-alphanumerisches Zeichen

Um die ausgewählten Kennworteigenschaften zu aktivieren, wählen Sie die Option *Komplexe Kennwörter verlangen* und klicken Sie auf *Übernehmen*.

Verzeichnisbenutzer vorab holen

Benutzer von eDirectory oder Active Directory können mit der UTM synchronisiert werden.Das bedeutet, dass Benutzerdefinitionen vorab auf UTM angelegt werden, sodass diese Benutzerdefinitionen bereits existieren, wenn sich ein Benutzer anmeldet. Der Synchronisierungsprozess kann wöchentlich oder täglich stattfinden.

Um das Vorabholen (engl. prefetching) zu aktivieren, nehmen Sie die folgenden Einstellungen vor:

Server: Die Auswahlliste enthält Server, die auf der Registerkarte *Server* angelegt wurden. Wählen Sie einen Server aus, für den Sie das Vorabholen aktivieren möchten.

Vorabholenintervall: Wählen Sie ein Intervall, um Benutzer vorab zu holen. Um die Synchronisierung wöchentlich stattfinden zu lassen, wählen Sie einen Wochentag, am dem die Synchronisierung beginnen soll.Um die Synchronisierung täglich stattfinden zu lassen, wählen Sie *Täglich*.

Vorabholenzeit: Wählen Sie eine Uhrzeit, zu der das Vorabholen von Benutzern stattfinden soll.

Gruppen: Geben Sie hier die Gruppen ein, die im Voraus angelegt werden sollen.Sie können den integrierten LDAP-Browser verwenden, um die Gruppen auszuwählen.

Aktiviere Backend-Synchronisierung bei Anmeldung (optional): Bei jedem Vorabholen wird die Option *Backend-Sync.* der betreffenden Benutzer (Registerkarte *Benutzer & Gruppen > Benutzer*) auf den hier festgelegten Wert gesetzt.Wenn die Option aktiv ist, wird also die Option *Backend-Sync.* der Benutzer aktiviert, und wenn die Option deaktiviert ist, wird die Option *Backend-Sync.* der Benutzer deaktiviert.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Jetzt vorab holen: Klicken Sie auf diese Schaltfläche, um das Vorabholen sofort zu starten.

Vorabholen-Live-Protokoll öffnen: Klicken Sie auf diese Schaltfläche, um das Vorabholen-Live-Protokoll zu öffnen.

Synchronisierung der Active-Directory-Gruppenmitgliedschaft

Verwenden Sie diese Option, um die Synchronisierung der Informationen zur AD-Gruppenmitgliedschaft im Hintergrund zu aktivieren.

Die UTM kann die Gruppenmitgliedschaftsinformationen regelmäßig synchronisieren und lokal zwischenspeichern, um den Active-Directory-Server zu entlasten. Wenn diese Option aktiviert ist, werden die Gruppenmitgliedschaftsinformationen mit dem konfigurierten Active-Directory-Single-Sign-On-Server synchronisiert.

Klicken Sie auf *Jetzt synchronisieren*, um die Gruppenmitgliedschaftsinformationen sofort zu synchronisieren.

6 Schnittstellen & Routing

In diesem Kapitel wird die Konfiguration von Schnittstellen und netzwerkspezifischen Einstellungen in Sophos UTM beschrieben. Die Seite *Netzwerkstatistik* in WebAdmin gibt einen Überblick über die zehn aktivsten Dienste und Quellhosts sowie die gleichzeitigen Verbindungen von heute. In jedem Abschnitt befindet sich ein Link auf die *Details*. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Berichte-Bereichs des WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Schnittstellen
- Bridging
- Dienstqualität (QoS)
- Uplink-Überwachung
- IPv6
- Statisches Routing
- Dynam. Routing (OSPF)
- Border Gateway Protocol
- Multicast Routing (PIM-SM)

6.1 Schnittstellen

Ein Gateway benötigt mindestens zwei Netzwerkkarten, um ein internes LAN mit einem externen Netzwerk (z. B. dem Internet) zu verbinden. In den folgenden Beispielen ist die Netzwerkkarte `eth0` immer die interne Netzwerkschnittstelle. Die Netzwerkkarte `eth1` ist als externe Netzwerkschnittstelle vorgesehen (z. B. zum Internet). Diese beiden Seiten werden auch Trusted bzw. Untrusted genannt.

Während der Installation werden die Netzwerkkarten automatisch erkannt. Wenn bei der Software-Appliance weitere Netzwerkkarten hinzugefügt werden, ist eine Neuinstallation des Sicherheitssystems notwendig. Nutzen Sie hierfür die Backup-Funktion, um nach der Neuinstallation Ihre aktuelle Systemkonfiguration einfach wieder einzuspielen.

Das Gateway muss die einzige Schnittstelle zwischen dem internen und dem externen Netzwerk sein. Alle Datenpakete müssen UTM passieren. Es wird dringend davon abgeraten, die internen und externen Schnittstellen über einen Hub oder Switch physikalisch zusammen auf ein Netzwerksegment zu legen, es sei denn, dieser ist als VLAN-Switch konfiguriert. Es kann zu falschen ARP-Auflösungen (Address Resolution Protocol) kommen (ARP-Clash) die nicht alle Betriebssysteme (z. B. die von Microsoft) verwalten können. Pro Gateway-Netzwerkschnittstelle muss daher auch ein physikalisches Netzwerk-Segment verwendet werden.

Im Menü *Schnittstellen* können Sie alle auf UTM installierten Netzwerkkarten sowie die Schnittstellen zum externen Netzwerk (Internet) und zu den internen Netzwerken (LAN, DMZ) konfigurieren und verwalten.

Hinweis – Beachten Sie bei der Planung Ihrer Netzwerktopologie und der Konfiguration von UTM, welche Netzwerkkarten Sie jeweils auf der Appliance auswählen. In den meisten Konfigurationen ist als Verbindung zum externen Netzwerk die Netzwerkschnittstelle mit SysID `eth1` vorgesehen. Für die spätere Installation eines Hochverfügbarkeitssystems (HA) benötigen Sie auf beiden Systemen eine Netzwerkkarte mit gleicher SysID. Weitere Informationen zur Installation des Hochverfügbarkeitssystems (HA-Failover) finden Sie auf der Seite *Verwaltung* > *Hochverfügbarkeit*.

In den folgenden Abschnitten wird erklärt, wie die verschiedenen Arten von Schnittstellen über die Registerkarten *Schnittstellen*, *Zusätzliche Adressen*, *Linkbündelung*, *Uplink-Ausgleich*, *Multipathregeln* und *Hardware* verwaltet und konfiguriert werden.

6.1.1 Schnittstellen

Auf der Registerkarte *Schnittstellen* können Sie die Netzwerkkarten und virtuellen Schnittstellen konfigurieren. In der Liste sind die bereits konfigurierten Netzwerkschnittstellen mit ihrem symbolischen Namen, Netzwerkkarte und aktueller Adresse aufgeführt. Der Status jeder Schnittstelle wird ebenso angezeigt. Durch Anklicken des Schiebereglers können Sie Schnittstellen aktivieren und deaktivieren. Beachten Sie, dass Schnittstellengruppen keinen Schieberegler haben.

Tipp – Durch einen Klick auf das Infosymbol einer Netzwerkschnittstelle in der Liste *Schnittstellen* werden Ihnen alle Konfigurationen angezeigt, in denen diese Schnittstelle verwendet wird.

Neu hinzugefügte Schnittstellen können am Anfang als *Aus* angezeigt werden, solange sich die Verbindung noch im Aufbau befindet. Sie können Schnittstellen bearbeiten oder löschen, indem Sie auf die entsprechenden Schaltflächen klicken.

6.1.1.1 Automatische Netzwerkschnittstellen-Definitionen

Jede Schnittstelle auf Ihrer UTM besitzt einen symbolischen Namen und eine Netzwerkkarte, der sie zugewiesen ist. Der symbolische Name wird verwendet, wenn Sie in anderen Konfigurationen auf diese Schnittstelle verweisen. Für jede Schnittstelle wird automatisch eine passende Gruppe von Netzwerkdefinitionen von UTM erstellt:

- Eine Definition, die die aktuelle IP-Adresse der Schnittstelle enthält, und deren Name sich aus dem Schnittstellennamen und dem Zusatz *(Address)* zusammensetzt.
- Eine Definition, die das Netzwerk enthält, mit dem die Schnittstelle verbunden ist, und deren Name sich aus dem Schnittstellennamen und dem Zusatz *(Network)* zusammensetzt. Diese Definition wird nicht für *Point-to-Point*-Schnittstellen (PPP) angelegt.
- Eine Definition, die die Broadcast-Adresse der Schnittstelle enthält, und deren Name sich aus dem Schnittstellennamen und dem Zusatz *(Broadcast)* zusammensetzt. Diese Definition wird nicht für *Point-to-Point*-Schnittstellen (PPP) angelegt.

Wenn die Schnittstelle eine dynamische Methode zur Adresszuweisung verwendet (wie z. B. DHCP oder Fernzuweisung), so werden diese Definitionen automatisch aktuell gehalten. Alle Einstellungen, die sich auf diese Definitionen beziehen, z. B. Firewall- und NAT-Regeln, werden ebenfalls automatisch mit den geänderten Adressen aktualisiert.

Eine Schnittstelle mit dem symbolischen Namen *Intern* ist bereits vordefiniert. Hierbei handelt es sich um die Administrationsschnittstelle, die typischerweise als interne Schnittstelle von UTM verwendet wird. Falls Sie sie umbenennen möchten, sollten Sie das direkt nach der Installation tun.

6.1.1.2 Arten von Schnittstellen

Die nachfolgende Liste gibt eine Übersicht darüber, welche Schnittstellentypen zur UTM hinzugefügt werden können und welche Hardware dafür benötigt wird:

Gruppe: Sie können Ihre Schnittstellen in Gruppen organisieren. Bei entsprechender Konfiguration können Sie eine Schnittstellengruppe anstelle mehrerer einzelner Schnittstellen wählen.

3G/UMTS: Diese Schnittstelle basiert auf einem USB-Modem-Stick.Bevor die Schnittstelle erstellt wird, muss der Stick eingesteckt und die UTM neu gestartet werden.

DSL (PPPoA/PPTP): PPP over ATM. Ein DSL-PPPoA-Gerät ermöglicht Ihnen, Ihr Gateway an *PPP-over-ATM*-kompatible DSL-Leitungen anzuschließen. Diese Geräte benutzen das PPTP-Protokoll, um IP-Pakete zu tunneln. Sie erfordern eine dedizierte Ethernet-Verbindung (sie können nicht mit anderen Schnittstellen auf derselben Hardware koexistieren). Sie müssen ein DSL-Modem an das Schnittstellennetzwerksegment anschließen. Die Netzwerkparameter für diese Gerätetypen können über eine entfernte Stelle zugewiesen werden (üblicherweise Ihr Internetanbieter). Außerdem müssen Sie einen Benutzernamen und Kennwort für das Konto bei Ihrem ISP angeben. Auch müssen Sie die IP-Adresse Ihres Modems angeben. Diese Adresse ist dem Modem normalerweise fest zugewiesen und kann nicht geändert werden. Um mit dem Modem kommunizieren zu können, müssen Sie eine NIC-IP-Adresse und eine Netzmaske eingeben. Die IP-Adresse des Modems muss sich dabei innerhalb des durch diese Parameter definierten Netzwerks befinden. Die *Ping-Adresse* muss ein Host am anderen Ende der PPTP-Verbindung sein, der die ICMP-Pinganfragen beantwortet. Sie können versuchen, den DNS-Server Ihres ISP dafür zu verwenden. Falls diese Adresse nicht über Ping erreicht werden kann, wird angenommen, dass die Verbindung tot ist, und die Verbindung wird neu aufgebaut.

DSL (PPPoE): PPP over Ethernet. Ein DSL-PPPoE-Gerät ermöglicht Ihnen, Ihr Gateway an *PPP-over-Ethernet*-kompatible DSL-Leitungen anzuschließen. Diese Geräte erfordern eine dedizierte Ethernet-Verbindung (sie können nicht mit anderen Schnittstellen auf derselben Hardware koexistieren). Sie müssen ein DSL-Modem an das Schnittstellennetzwerksegment anschließen. Die Netzwerkparameter für diese Gerätetypen können über eine entfernte Stelle zugewiesen werden (üblicherweise Ihr Internetanbieter). Außerdem müssen Sie einen Benutzernamen und Kennwort für das Konto bei Ihrem ISP angeben.

Ethernet-DHCP: Hierbei handelt es sich um eine Standard-Ethernet-Schnittstelle mit DHCP.

Ethernet-Statisch: Dabei handelt es sich um eine normale Ethernet-Schnittstelle mit einer Bandbreite von 10, 100 oder 1000 Mbit/s.

Ethernet-VLAN: VLAN (Virtual LAN) ist eine Methode, um mehrere Schicht-2-getrennte Netzwerksegmente auf einer einzigen Hardwareschnittstelle zu ermöglichen. Jedes Segment wird durch eine VLAN-ID (auch engl. tag genannt) identifiziert, wobei es sich um eine einfache Ganzzahl (engl. integer) handelt. Wenn Sie eine VLAN-Schnittstelle hinzufügen, erzeugen Sie damit ein Hardware-Gerät, das dazu verwendet werden kann, auch zusätzliche Schnittstellen (Aliasse) hinzuzufügen. PPPoE- und PPPoA-Geräte können nicht über VLAN-virtuelle Hardware betrieben werden.

Modem (PPP): Mit diesem Schnittstellentyp können Sie die UTM über ein PPP-Modem mit dem Internet verbinden. Für die Konfiguration benötigen Sie eine serielle Schnittstelle und ein

externes Modem auf der UTM. Darüber hinaus benötigen Sie DSL-Zugangsdaten wie Benutzername und Kennwort. Diese Daten erhalten Sie von Ihrem Internetanbieter.

Über flexible Slots

Bestimmte Typen von Sophos-Hardware-Appliances besitzen so genannte Slots, über die die Schnittstellen-Hardware einfach verändert werden kann, indem Slot-Module flexibel eingesteckt oder ausgetauscht werden. Wenn diese Art von Hardware verwendet wird, zeigt der WebAdmin die Slot-Information zusammen mit den Hardware-Schnittstellen an. Dies sieht beispielsweise so aus:*eth1 [A6] Intel Corporation 82576 Gigabit Network Connection*, wobei die Slot-Information in den eckigen Klammern steht, und *A6* der sechste Port in Slot A ist. Derzeit sind bis zu drei Slots möglich, die von A bis C benannt sind und jeweils bis zu acht Ports besitzen können. Integrierte Schnittstellenkarten heißen *[MGMT1]* und *[MGMT2]*.

Slot-Informationen werden an den folgenden Stellen des WebAdmin angezeigt:

- *Schnittstellen & Routing* > *Schnittstellen* > *Schnittstellen*
- *Schnittstellen & Routing* > *Schnittstellen* > *Hardware*
- Im gesamten WebAdmin in *Hardware*-Auswahllisten und Listen, in denen Hardwareschnittstellen-Informationen angezeigt werden

Aktuelle Informationen darüber, welche Appliance-Typen flexible Slots besitzen, finden Sie auf der Sophos UTMWebseite.

6.1.1.3 Gruppe

Zwei oder mehr Schnittstellen lassen sich zu einer Gruppe zusammenfassen. Gruppen erleichtern die Konfiguration. Beim Erstellen von Multipathregeln müssen Sie eine Gruppe konfigurieren, wenn Sie den Datenverkehr auf eine definierte Gruppe von Uplink-Schnittstellen verteilen möchten, anstatt alle Uplink-Schnittstellen zu verwenden.

Um eine *Gruppen*-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
   Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *Gruppe* aus der Auswahlliste aus.

   Schnittstellen: Fügen Sie die gewünschten Schnittstellen zur Gruppe hinzu.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die Gruppe wird zur Schnittstellenliste hinzugefügt. Gruppen haben keinen Status.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.4 3G/UMTS

Sophos UTMunterstützt Netzwerkverbindungen über 3G/UMTS-USB-Sticks.

Um eine 3G/UMTS-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
   Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *3G/UMTS* aus der Auswahlliste aus.

   Hardware: Wählen Sie einen USB-Modem-Stick aus der Auswahlliste aus. Beachten Sie, dass nach dem Anschluss des USB-Sticks ein Neustart erforderlich ist.

   Netzwerk: Wählen Sie den Typ des Mobilfunknetzes aus (entweder *GSM/W-CDMA*, *CDMA* oder *LTE*).

   IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie das Standardgateway Ihres Anbieters nutzen möchten.

   PIN (optional): Geben Sie die PIN der SIM-Karte ein, falls eine PIN konfiguriert ist.

   APN automatisch wählen: (optional): Standardmäßig wird der APN (Access Point Name) vom USB-Modem-Stick abgerufen. Wenn Sie die Auswahl dieses Kontrollkästchens deaktivieren, müssen Sie die APN-Informationen in das Feld *APN* eingeben.

   Benutzername/Kennwort (optional): Geben Sie, sofern erforderlich, einen Benutzernamen und ein Kennwort für das Mobilfunknetz ein.

Einwahlkennung (optional): Sollte Ihr Dienstanbieter eine spezifische Einwahlkennung verwenden, müssen Sie diese hier eingeben.Der Standard ist `*99#`.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Init-Kennung: Geben Sie die Kennung zur Initialisierung des USB-Modem-Sticks ein. Beachten Sie, dass die Init-Kennung eventuell dem USB-Modem-Stick angepasst werden muss. In diesem Fall entnehmen Sie die Init-Kennung dem zugehörigen Handbuch des USB-Modem-Sticks. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld *ATZ* ein.

   Rückstellung: Geben Sie die Kennung zur Rückstellung des USB-Modem-Sticks ein. Beachten Sie auch hier, dass die Rückstellungskennung eventuell dem USB-Modem-Stick angepasst werden muss. In diesem Fall entnehmen Sie diese dem zugehörigen Handbuch des USB-Modem-Sticks. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld *ATZ* ein.

   MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für die Schnittstellenart *3G/UMTS* auf 1500 Byte voreingestellt.

   Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

   Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

4. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
   Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

   Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.5 Ethernet-Statisch

Um eine Netzwerkkarte für eine statische Ethernet-Verbindung zu einem internen oder externen Netzwerk zu konfigurieren, muss die Netzwerkkarte mit einer IP-Adresse und einer Netzmaske konfiguriert werden.

Um eine Ethernet-Statisch-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.

1. Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *Ethernet-Statisch* aus der Auswahlliste aus.

   Hardware: Wählen Sie eine Schnittstelle aus der Auswahlliste aus.

   > **Tipp –** Wählen Sie als Schnittstelle zum externen Netzwerk (z. B. zum Internet) die Netzwerkkarte mit der SysID eth1 aus. Beachten Sie, dass eine Netzwerkkarte nicht gleichzeitig als *Ethernet-Statisch*-Schnittstelle und als *PPP-over-Ethernet (PPPoE-DSL)* oder *PPTP-over-Ethernet (PPPoA-DSL)* genutzt werden kann.

   IPv4/IPv6 Adresse: Geben Sie die IP-Adresse für die Schnittstelle ein.

Netzmaske: Wählen Sie eine Netzmaske (IPv4) und/oder geben Sie eine IPv6-Netzmaske ein.

IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie ein statisches Standardgateway verwenden wollen.

Standard-GW-IP (optional): Tragen Sie hier die IP-Adresse des Standardgateways ein.

Hinweis – Eine Schnittstelle kann gleichzeitig eine IPv4- und eine IPv6-Adresse besitzen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für die Schnittstellenart *Ethernet-Statisch* auf 1.500 Byte voreingestellt.

   Proxy-ARP: Wählen Sie diese Option aus, um die Proxy-ARP-Funktion zu aktivieren. Standardmäßig ist die Funktion *Proxy-ARP* deaktiviert.
   Diese Funktion ist für Schnittstellen vom Typ Broadcast verfügbar. Wenn diese Funktion aktiviert ist, wird die UTM über diese Schnittstelle Datenverkehr stellvertretend für andere Hosts annehmen und diesen entsprechend weiterleiten. Diese Aufgabe übernimmt die Firewall für alle Hosts, zu denen sie eine direkte Schnittstellenroute besitzt. Das ermöglicht Ihnen, ein „transparentes“ Netzwerk-Bridging einzurichten ohne auf die Firewall-Eigenschaften zu verzichten. Ein anderer Anwendungsfall für diese Funktion ist, wenn der Router Ihres Anbieters (ISP) Ihr „offizielles“ Netzwerk einfach auf seine Ethernetschnittstelle setzt (anstelle eine Host-Route zu verwenden).

   Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite

des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

4. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
   Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

   Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.6 Ethernet-VLAN

Um eine Verbindung zwischen der UTM und den virtuellen LANs herzustellen, benötigt das System eine Netzwerkkarte mit einem Tag-fähigen Treiber. Ein -Tag ist ein kleiner 4-Byte-Header, der an den Ethernet-Header von Paketen angefügt wird. Das Tag enthält die Nummer des VLAN, für das dieses Paket bestimmt ist: Die VLAN-Nummer besteht aus 12 Bit, dadurch sind 4.095 verschiedene virtuelle LANs möglich. Diese VLAN-Nummer wird in WebAdmin als *VLAN-Tag* oder VLAN-ID bezeichnet.

> **Hinweis –**Sophos verwaltet eine Liste der unterstützten, Tag-fähigen Netzwerkkarten. Die *Hardwarekompatibilitätsliste* (Hardware Compatibility List; HCL) steht in SophosKnowledgebase zur Verfügung. Verwenden Sie „HCL“ als Suchbegriff, um die entsprechende Seite zu finden.

Um eine Ethernet-VLAN-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.

1. Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *Ethernet-VLAN* aus der Auswahlliste aus.

   Hardware: Wählen Sie eine Schnittstelle aus der Auswahlliste aus.

   VLAN-Tag: Tragen Sie das VLAN-Tag für diese Schnittstelle ein.

   IPv4/IPv6 Adresse: Geben Sie die IP-Adresse für die Schnittstelle ein.

   Netzmaske: Wählen Sie eine Netzmaske (IPv4) und/oder geben Sie eine IPv6-Netzmaske ein.

   IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie ein statisches Standardgateway verwenden wollen.

   Standard-GW-IP (optional): Tragen Sie hier die IP-Adresse des Standardgateways ein.

   Hinweis – Eine Schnittstelle kann gleichzeitig eine IPv4- und eine IPv6-Adresse besitzen.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für den Schnittstellentyp *Ethernet-VLAN* auf 1.500 Byte voreingestellt.

   Proxy-ARP: Wählen Sie diese Option aus, um die Proxy-ARP-Funktion zu aktivieren. Standardmäßig ist die Funktion *Proxy-ARP* deaktiviert.
   Diese Funktion ist für Schnittstellen vom Typ Broadcast verfügbar. Wenn diese Funktion aktiviert ist, wird die UTM über diese Schnittstelle Datenverkehr stellvertretend für

andere Hosts annehmen und diesen entsprechend weiterleiten. Diese Aufgabe übernimmt die Firewall für alle Hosts, zu denen sie eine direkte Schnittstellenroute besitzt. Das ermöglicht Ihnen, ein „transparentes“ Netzwerk-Bridging einzurichten ohne auf die Firewall-Eigenschaften zu verzichten. Ein anderer Anwendungsfall für diese Funktion ist, wenn der Router Ihres Anbieters (ISP) Ihr „offizielles“ Netzwerk einfach auf seine Ethernetschnittstelle setzt (anstelle eine Host-Route zu verwenden).

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

4. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
   Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

   Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.7 Ethernet-DHCP

Um eine *Ethernet-DHCP*-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.

1. Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *Ethernet-DHCP* aus der Auswahlliste aus.

   Hardware: Wählen Sie eine Schnittstelle aus der Auswahlliste aus.

   Tipp – Wählen Sie als Schnittstelle zum externen Netzwerk (z. B. zum Internet) die Netzwerkkarte mit der SysID `eth1` aus. Beachten Sie, dass eine Netzwerkkarte nicht gleichzeitig als *Ethernet-DHCP* und als *PPP-over-Ethernet* (PPPoE-DSL) oder *PPTP-over-Ethernet* (PPPoA-DSL) genutzt werden kann.

   IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie das Standardgateway Ihres Anbieters nutzen möchten.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Hostname: Wenn Ihr ISP den Hostnamen Ihres Systems benötigt, geben Sie ihn hier ein.

   MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für den Schnittstellentyp *Ethernet-DHCP* auf 1.500 Byte voreingestellt.

   Proxy-ARP: Wählen Sie diese Option aus, um die Proxy-ARP-Funktion zu aktivieren. Standardmäßig ist die Funktion *Proxy-ARP* deaktiviert.
   Diese Funktion ist für Schnittstellen vom Typ Broadcast verfügbar. Wenn diese Funktion aktiviert ist, wird die UTM über diese Schnittstelle Datenverkehr stellvertretend für andere Hosts annehmen und diesen entsprechend weiterleiten. Diese Aufgabe übernimmt die Firewall für alle Hosts, zu denen sie eine direkte Schnittstellenroute besitzt. Das ermöglicht Ihnen, ein „transparentes“ Netzwerk-Bridging einzurichten ohne auf die Firewall-Eigenschaften zu verzichten. Ein anderer Anwendungsfall für diese Funktion ist,

wenn der Router Ihres Anbieters (ISP) Ihr „offizielles“ Netzwerk einfach auf seine Ethernetschnittstelle setzt (anstelle eine Host-Route zu verwenden).

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

4. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
   Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

   Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.8 DSL (PPPoE)

Für diese Konfiguration benötigen Sie DSL-Zugangsdaten wie Benutzername und Kennwort. Die Zugangsdaten erhalten Sie von Ihrem ISP.VDSL wird ebenfalls von dieser Schnittstellenart unterstützt.

Hinweis – Die UTM ist nach Aktivierung der DSL-Verbindung täglich 24 Stunden mit Ihrem Internetanbieter verbunden. Sie sollten daher sicherstellen, dass Ihr Anbieter die Verbindung als Flatrate oder bandbreitenbasiert abrechnet und nicht anhand der Verbindungsdauer.

Um eine DSL-(PPPoE)-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
   Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *DSL (PPPoE)* aus der Auswahlliste aus.

   Hardware: Wählen Sie eine Schnittstelle aus der Auswahlliste aus.

   VDSL: Wählen Sie diese Option (nur) aus, wenn es sich bei der Verbindung um eine VDSL-Verbindung handelt.Der *MTU*-Wert ändert sich auf `1476`.

   Statische PPPoE-IP (optional): Markieren Sie dieses Auswahlfeld, wenn Sie von Ihrem Internetanbieter eine statische IP-Adresse zugewiesen bekommen haben, und geben Sie die IP-Adresse und die dazugehörige Netzmaske in die erscheinenden Textfelder ein.

   - **IPv4/IPv6 Adresse:** Geben Sie die zusätzliche IP-Adresse für die Schnittstelle ein.

   - **Netzmaske:** Wählen Sie aus der Auswahlliste eine Netzmaske aus und/oder tragen Sie eine IPv6-Netzmaske ein.

   Hinweis – Eine Schnittstelle kann gleichzeitig eine IPv4- und eine IPv6-Adresse besitzen.

   IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie das Standardgateway Ihres Anbieters nutzen möchten.

   Benutzername: Tragen Sie den Benutzernamen ein, den Sie von Ihrem Anbieter erhalten haben.

   Kennwort: Tragen Sie das Kennwort ein, das Sie von Ihrem Internetanbieter erhalten haben.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der

Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für die Schnittstellenart *DSL (PPPoE)* auf 1492 Byte voreingestellt.

VLAN-Tag (nur wenn *VDSL* aktiv ist): Geben Sie den VLAN-Tag ein, der zu den PPPoE-Paketen hinzugefügt werden soll. Das korrekte Tag erfahren Sie von Ihrem VDSL-Provider. Der Standardwert 7 wird derzeit für die PPPoE-Verbindung der Deutschen Telekom verwendet.

Tägliche Wiedereinwahl: Definieren Sie hier, zu welcher Uhrzeit die Verbindung beendet und wieder neu aufgebaut werden soll. Sie können zwischen *Nie* und einer beliebigen Uhrzeit wählen.

Verzögerte Wiedereinwahl: Definieren Sie hier die Zeitverzögerung für die Wiedereinwahl. Standardmäßig beträgt sie *5 Sekunden*. Sollte Ihr Anbieter eine längere Verzögerung erfordern, können Sie den Wert auf *Eine Minute* oder *Fünfzehn Minuten* setzen.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Multilink: Wenn die Option aktiv ist, können Sie mehrere PPP-Verbindungen bündeln. Eine Multilink-PPP-Verbindung ist nur möglich, wenn Ihr ISP Multilink PPP unterstützt.

Multilink-Slaves: Wählen Sie die Schnittstellen, die Sie mit der oben gewählten Hardware zu einem Multilink bündeln möchten.

4. **Klicken Sie auf *Speichern*.**

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

   Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.9 DSL (PPPoA/PPTP)

Für die Konfiguration einer *PPP-over-ATM-Verbindung* (PPPoA) benötigen Sie auf der UTM eine freie Ethernet-Netzwerkkarte und ein externes ADSL-Modem mit Ethernet-Anschluss. Die Verbindung zum Internet erfolgt über zwei Teilstrecken. Zwischen der UTM und dem ADSL-Modem erfolgt die Verbindung mit dem *Protokoll PPTP over Ethernet*. Die Verbindung vom ADSL-Modem zum Internetanbieter (ISP) erfolgt mit dem ADSL-Einwahlprotokoll *PPP over ATM*.

Für diese Konfiguration benötigen Sie DSL-Zugangsdaten wie Benutzername und Kennwort. Die Zugangsdaten erhalten Sie von Ihrem ISP.

Hinweis – Die UTM ist nach Aktivierung der DSL-Verbindung täglich 24 Stunden mit Ihrem Internetanbieter verbunden. Sie sollten daher sicherstellen, dass Ihr Anbieter die Verbindung als Flatrate oder bandbreitenbasiert abrechnet und nicht anhand der Verbindungsdauer.

Um eine DSL-(PPPoA/PPTP)-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.

1. Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *DSL (PPPoA/PPTP)* aus der Auswahlliste aus.

Hardware: Wählen Sie eine Schnittstelle aus der Auswahlliste aus.

IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie das Standardgateway Ihres Anbieters nutzen möchten.

Benutzername: Tragen Sie den Benutzernamen ein, den Sie von Ihrem Anbieter erhalten haben.

Kennwort: Tragen Sie das Kennwort ein, das Sie von Ihrem Internetanbieter erhalten haben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
Modem-IP: Tragen Sie die IP-Adresse des ADSL-Modems ein. Diese Adresse wird in der Regel vom Anbieter oder von der Hardware mitgeliefert und kann nicht geändert werden. Beispiel: `10.0.0.138` (bei AonSpeed).

NIC-Adresse: Tragen Sie die IP-Adresse für die Netzwerkkarte auf der UTM ein, die an das Modem angeschlossen ist. Diese Adresse muss im selben Subnetz liegen wie die IP-Adresse des Modems. Beispiel: `10.0.0.140` (bei AonSpeed).

NIC-Netzmaske: Tragen Sie die Netzmaske ein.
Beispiel: `255.255.255.0` (bei AonSpeed).

Ping-Adresse (optional): Tragen Sie die IP-Adresse eines Hosts im Internet ein, der auf ICMP-Ping-Anfragen antwortet. Um die Verbindung zwischen der UTM und dem externen Netzwerk zu testen, geben Sie eine IP-Adresse eines Hosts am anderen Ende der PPTP-Verbindung an. Sie können versuchen, den DNS-Server Ihres ISP dafür zu verwenden. Die UTM sendet Ping-Anfragen zu diesem Host: Falls das System von diesem Host keine Antwort erhält, ist die Verbindung nicht intakt.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für die Schnittstellenart *DSL (PPPoA)* auf 1492 Byte voreingestellt.

Tägliche Wiedereinwahl: Definieren Sie hier, zu welcher Uhrzeit die Verbindung beendet und wieder neu aufgebaut werden soll. Sie können zwischen *Nie* und einer beliebigen Uhrzeit wählen.

Verzögerte Wiedereinwahl: Definieren Sie hier die Zeitverzögerung für die Wiedereinwahl. Standardmäßig beträgt sie *5 Sekunden*. Sollte Ihr Anbieter eine längere Verzögerung erfordern, können Sie den Wert auf *Eine Minute* oder *Fünfzehn Minuten* setzen.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

4. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
   Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

   Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.1.10 Modem (PPP)

Für die Konfiguration benötigen Sie eine serielle Schnittstelle und ein externes PPP-Modem auf der UTM. Darüber hinaus benötigen Sie DSL-Zugangsdaten wie Benutzername und Kennwort. Diese Daten erhalten Sie von Ihrem Internetanbieter.

Um eine *Modem-(PPP)*-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
   Das Dialogfeld *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Schnittstelle ein.

   Typ: Wählen Sie *Modem (PPP)* aus der Auswahlliste aus.

   Hardware: Wählen Sie eine Schnittstelle aus der Auswahlliste aus.

   IPv4/IPv6 Standard-GW (optional): Wählen Sie diese Option, wenn Sie das Standardgateway Ihres Anbieters nutzen möchten.

   Benutzername: Tragen Sie den Benutzernamen ein, den Sie von Ihrem Anbieter erhalten haben.

   Kennwort: Tragen Sie das Kennwort ein, das Sie von Ihrem Internetanbieter erhalten haben.

   Einwahlkennung: Geben Sie die Telefonnummer ein.Beispiel: `5551230`

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Geschwindigkeit: Stellen Sie hier die Geschwindigkeit in Bit pro Sekunde für die Verbindung zwischen der UTM und dem Modem ein. Übliche Werte sind 57.600 Bit/s und 115.200 Bit/s.

   Datenflusskontrolle: Stellen Sie die Methode zur Kontrolle des Datenflusses ein. Wenn die Daten über die serielle Verbindung laufen, kann es vorkommen, dass das System die ankommenden Daten nicht schnell genug verarbeiten kann. Um sicherzustellen, dass keine Daten verloren gehen, ist eine Methode zur Kontrolle des Datenflusses notwendig. Bei der seriellen Verbindung sind zwei Methoden verfügbar:

   - *Hardware*-Signale
   - *Software*-Signale

   Da bei einer PPP-Verbindung alle acht Bit der Leitung verwendet werden und sich in den übertragenen Daten die Byte der Steuerzeichen *Control S* und *Control Q* befinden, empfehlen wir, die Voreinstellung *Hardware* beizubehalten und ein entsprechendes serielles Verbindungskabel zu verwenden.

Init-Kennung: Tragen Sie die Kennung zur Initialisierung des Modems ein. Beachten Sie, dass die Init-Kennung (init string) eventuell dem Modem angepasst werden muss. In diesem Fall entnehmen Sie die Init-Kennung dem zugehörigen Modem-Handbuch. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld *ATZ* ein.

Rückstellung: Tragen Sie die Rückstellungskennung (reset string) für das Modem ein. Beachten Sie auch hier, dass die Rückstellungskennung eventuell dem Modem angepasst werden muss. In diesem Fall entnehmen Sie diese dem zugehörigen Modem-Handbuch. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld *ATZ* ein.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. Maximum Transmission Unit) für die Schnittstelle in Byte an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Ein MTU-Wert, der größer als 1500 Byte ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden. Der MTU-Wert ist für die Schnittstellenart *Modem (PPP)* auf 1492 Byte voreingestellt.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard dies widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die maximale Bandbreite des Uplinks in entweder MB/s oder KB/s angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in MB/s oder KB/s angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

4. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

5. **Aktivieren Sie die Schnittstelle.**
   Klicken Sie auf den Schieberegler, um die Schnittstelle zu aktivieren.

Die Schnittstelle ist jetzt aktiv (Schieberegler ist grün). Die Schnittstelle wird zunächst möglicherweise noch als *Aus* (nicht verbunden) angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die neue Schnittstelle ist betriebsbereit, wenn die Statusmeldung *An* angezeigt wird.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, wählen Sie im Filtermenü die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.2 Zusätzliche Adressen

Eine Netzwerkkarte kann mit zusätzlichen IP-Adressen konfiguriert werden (auch *Aliasse* genannt). Diese Funktion wird benötigt, um auf einer physikalischen Netzwerkkarte mehrere logische Netzwerke zu verwalten. Sie kann auch verwendet werden, um UTM im Zusammenhang mit NAT (Network Address Translation) zusätzliche Adressen zuzuweisen.

Um zusätzliche Adressen auf einer Netzwerkkarte zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zusätzliche Adressen* auf *Neue zusätzliche Adresse*.**
   Das Dialogfeld *Neue zusätzliche Adresse erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die neue zusätzliche Adresse ein.

   Auf Schnittstelle: Wählen Sie im Auswahlmenü die Netzwerkkarte aus, der die Adresse zugewiesen werden soll.

   IPv4/IPv6 Adresse: Geben Sie die zusätzliche IP-Adresse für die Schnittstelle ein.

   Netzmaske: Wählen Sie aus der Auswahlliste eine Netzmaske aus und/oder tragen Sie eine IPv6-Netzmaske ein.

   Hinweis – Eine Schnittstelle kann gleichzeitig eine IPv4- und eine IPv6-Adresse besitzen.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung wird die neue Schnittstelle in der Schnittstellen-Liste angezeigt. Die Schnittstelle ist noch nicht aktiv (Schieberegler ist grau).

4. **Aktivieren Sie die zusätzliche Adresse.**
   Aktivieren Sie die zusätzliche Adresse durch einen Klick auf den Schieberegler.

   Die zusätzliche Adresse ist nun eingeschaltet (Schieberegler zeigt Grün). Die zusätzliche Adresse wird möglicherweise dennoch als *Aus* angezeigt. Das System benötigt kurze Zeit, um die Einstellungen zu konfigurieren und zu laden. Die zusätzliche Adresse ist vollständig einsatzbereit, sobald die Meldung *An* angezeigt wird.

Um eine zusätzliche Adresse zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.3 Linkbündelung

Linkbündelung (engl. Link Aggregation) (auch Kanalbündelung, port trunking oder NIC bonding) fasst mehrere parallele Ethernet-Verbindungen zu einer logischen Verbindung mit einer IP-Adresse zusammen. Die gebündelten Ports werden von Ihrem System als eine einzige IP-Adresse wahrgenommen. Mit Linkbündelung lässt sich einerseits die Bandbreite über die Kapazität einer einzelnen NIC hinaus vervielfachen, andererseits bietet es durch die redundanten Verbindungen eine einfache Ausfallsicherung (Failover) und Fehlertoleranz für den Fall, dass ein Port oder Switch ausfällt. Der gesamte Datenverkehr, der über den ausgefallenen Port oder Switch lief, wird automatisch auf die übrigen Ports oder Switches umgeleitet. Eine solche Ausfallsicherung ist für das System, das diese Verbindung benutzt, völlig transparent.

Hinweis – In einer Hochverfügbarkeitsumgebung können die einzelnen Ethernet-Verbindungen sogar auf verschiedenen HA-Einheiten sein.

Sie können bis zu vier verschiedene Linkbündelungsgruppen definieren. Eine Gruppe kann aus einer oder mehreren Schnittstellen bestehen.

Um eine Linkbündelungsgruppe (LAG) zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Wählen Sie für jede LAG, welche Schnittstellen Sie hinzufügen wollen.**
   Eine Gruppe kann aus einer konfigurierten Schnittstelle und/oder einer oder mehreren unkonfigurierten Schnittstellen bestehen.

Um eine konfigurierte Schnittstelle zu verwenden, wählen Sie diese aus der Auswahlliste *Konvertierungsschnittstelle* aus. Um unkonfigurierte Schnittstellen zu verwenden, markieren Sie die entsprechenden Auswahlkästchen.

2. **Aktivieren Sie die LAG.**
   Aktivieren Sie die LAG durch einen Klick auf die Schaltfläche *Diese Gruppe aktivieren*.

   Sobald die Linkbündelungsgruppe konfiguriert ist, steht eine neue LAG-Schnittstelle (z. B. `lag0`) zur Verfügung, die ausgewählt werden kann, wenn Sie eine neue Schnittstellendefinition auf der Registerkarte *Schnittstellen* anlegen. Für eine LAG können die folgenden Schnittstellenarten konfiguriert werden:

   - Ethernet-Statisch
   - Ethernet-VLAN
   - Ethernet-DHCP
   - Alias-Schnittstellen

Um eine LAG zu deaktivieren, entfernen Sie die Häkchen aus den Auswahlkästchen, die Teil dieser LAG sind, klicken auf *Diese Gruppe aktualisieren* und bestätigen den Warnhinweis.Der Status der LAG wird auf der Registerkarte *Support* > *Erweitert* > *Schnittstellen* angezeigt.

6.1.4 Uplink-Ausgleich

Mit der Uplink-Ausgleich-Funktion können Sie mehrere Internetverbindungen zusammenfassen, entweder um Zusatzverbindungen bei einem Ausfall zu haben oder um die Last auf mehrere Verbindungen zu verteilen. Die Kombination von bis zu 32 unterschiedlichen Internetverbindungen wird unterstützt. Beachten Sie, dass mit dem BasicGuard-Abonnement nur zwei Uplinks kombiniert werden können.

Der Uplink-Ausgleich ist automatisch aktiviert, wenn Sie einer Schnittstelle zusätzlich zu einer bereits vorhandenen Schnittstelle mit Standardgateway ein Standardgateway zuweisen. Alle Schnittstellen mit Standardgateway werden zum Feld *Aktive Schnittstellen* hinzugefügt und der Uplink-Ausgleich wird ab diesem Zeitpunkt automatisch durchgeführt. Weitere Schnittstellen mit Standardgateway werden ebenfalls automatisch hinzugefügt.

Auf der Registerkarte *Multipathregeln* können Sie konkrete Regeln für den auszugleichenden Datenverkehr definieren.

Um den Uplink-Ausgleich manuell einzurichten, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den Uplink-Ausgleich.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Uplink-Ausgleich* kann nun bearbeitet werden.

2. **Wählen Sie aktive Schnittstellen aus.**
   Fügen Sie eine oder mehrere Schnittstellen hinzu, indem Sie auf das Ordnersymbol klicken und danach Schnittstellen aus der Objektleiste herüberziehen. Bei mehreren Schnittstellen wird der von Clients kommende Verkehr über die Quelle ausgeglichen, d. h., der gesamte von einer Quelle kommende Verkehr verwendet dieselbe Schnittstelle, während Verkehr von anderen Quellen zu anderen Schnittstellen geleitet werden kann. Wenn eine der Schnittstellen nicht erreichbar ist, wird der Verkehr von der/den verbleibenden Schnittstelle(n) übernommen.

   Hinweis – Wenn der Uplink-Ausgleich automatisch aktiviert wurde, enthält die Liste *Aktive Schnittstellen* zunächst bereits alle Schnittstellen mit Standardgateway. Wenn Sie eine Schnittstelle aus der Liste entfernen, wird das Auswahlkästchen *Standardgateway* der Schnittstelle automatisch deaktiviert. Daher muss jede Schnittstelle mit Standardgateway entweder auf dieser Liste oder im Feld *Standby-Schnittstellen* unten aufgeführt sein. Sie können jedoch Schnittstellen ohne Standardgateway hinzufügen und die Standardgatewayadresse später eingeben.

   Hinweis – Die Reihenfolge der Schnittstellen ist wichtig: In Konfigurationen, in denen nur eine Schnittstelle verwendet werden kann, sowie für Pakete, die von UTM selbst gesendet werden, wird standardmäßig die erste verfügbare aktive Schnittstelle verwendet. Sie können die Reihenfolge der Schnittstellen mit Hilfe der Sortieren-Symbole ändern.

   Über das Symbol „Planer bearbeiten“ in der Kopfzeile des Feldes können Sie das Verteilungsverhalten und die Schnittstellenbindung der aktiven Schnittstellen festlegen:

   Gewichtung: Die Gewichtung kann auf einen Wert zwischen 0 und 100 festgelegt werden und gibt an, wie viel Datenverkehr eine Schnittstelle im Vergleich zu allen anderen Schnittstellen verarbeitet. Hierfür wird ein gewichteter Round-Robin-Algorithmus verwendet. Ein höherer Wert bedeutet, dass mehr Datenverkehr über die jeweilige Schnittstelle geroutet wird. Die Werte werden im Verhältnis zueinander bewertet, daher muss ihre Summe nicht 100 ergeben. So ist z. B. eine Konfiguration möglich, bei der

Schnittstelle 1 den Wert 100, Schnittstelle 2 den Wert 50 und Schnittstelle 3 den Wert 0 hat. Dabei bearbeitet Schnittstelle 2 nur halb so viel Datenverkehr wie Schnittstelle 1, während Schnittstelle 3 nur aktiv wird, wenn keine der anderen Schnittstellen verfügbar ist. Der Wert Null bedeutet, dass grundsätzlich eine andere Schnittstelle mit höherem Wert gewählt wird, wenn diese verfügbar ist.

Bindung: Schnittstellen-Bindung ist ein Verfahren, das gewährleistet, dass Datenverkehr mit bestimmten Attributen immer über dieselbe Uplink-Schnittstelle geroutet wird. Die Bindung hat eine Zeitbeschränkung von einer Stunde.

3. **Ausgewählte Standby-Schnittstellen** (optional).
   Hier können Sie optional Ersatz-Schnittstellen hinzufügen, die nur in Aktion treten, wenn alle aktiven Schnittstellen unerreichbar sind. In diesem Fall wird die erste verfügbare Standby-Schnittstelle entsprechend der gegebenen Reihenfolge verwendet. Sie können die Reihenfolge der Schnittstellen mit Hilfe der Sortieren-Symbole ändern.

4. **Überwachungseinstellungen ändern** (optional).
   Automatische Überwachung ist standardmäßig aktiviert, um ein mögliches Versagen einer Schnittstelle zu entdecken. Dies bedeutet, dass der Zustand aller Uplink-Schnittstellen überwacht wird, indem ein bestimmter Host im Internet in einem Abstand von 15 Sekunden angesprochen wird. Standardmäßig ist der überwachende Host der dritte Pings zulassende Hop auf dem Weg zu einem der Root-DNS-Server. Sie können die Hosts zum Überwachen der Server auch selbst bestimmen. Für diese Hosts können Sie einen anderen Dienst als Ping auswählen und Überwachungsintervall und -zeitüberschreitung anpassen:

   Sobald die überwachenden Hosts keine Antwort mehr senden, wird die entsprechende Schnittstelle als tot betrachtet und nicht mehr für die Verteilung verwendet. Auf dem Dashboard wird dann in der Spalte *Link* der Schnittstelle *Fehler* angezeigt.

   Hinweis – Automatisch werden dieselben Überwachungseinstellungen sowohl für die Uplink-Überwachung (*Uplink-Überwachung* > *Erweitert*) als auch für den Uplink-Ausgleich (*Schnittstellen* > *Uplink-Ausgleich*) verwendet.

   Um eigene Hosts für die Überwachung des Server-Pools zu definieren, gehen Sie folgendermaßen vor:

   1. **Deaktivieren Sie das Auswahlkästchen *Automatische Überwachung*.**
      Das Feld *Überwachende Hosts* kann nun bearbeitet werden.

2. **Fügen Sie die überwachenden Hosts hinzu.**
   Wählen Sie einen oder mehrere Hosts aus oder fügen Sie Hosts hinzu, die anstelle einer zufälligen Auswahl an Hosts die Überwachung übernehmen sollen. Wenn eine Schnittstelle von mehr als einem Host überwacht wird, wird sie nur als tot betrachtet, wenn keiner der überwachenden Hosts in der festgelegten Zeitspanne antwortet. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   Hinweis – Wenn ein ausgewählter Host an eine Schnittstelle gebunden ist, wird er nur zur Überwachung dieser Schnittstelle verwendet. Ist ein Host nicht an eine Schnittstelle gebunden, wird er zur Überwachung aller Schnittstellen verwendet. Schnittstellen, die nicht von den ausgewählten Hosts überwacht werden, werden automatisch überwacht.

   Klicken Sie auf das Symbol Überwachungseinstellungen bearbeiten im Kopf des Feldes, um die Überwachungsdetails festzulegen:

   Überwachungstyp: Wählen Sie das Dienstprotokoll für die Überwachungsprüfungen aus. Wählen Sie für die Dienstüberwachung entweder *TCP* (TCP-Verbindungsaufbau), *UDP* (UDP-Verbindungsaufbau), *Ping* (ICMP-Ping), *HTTP Host* (HTTP-Anfragen) oder *HTTPS Host* (HTTPS-Anfragen). Wenn Sie *UDP* verwenden, wird zunächst eine Ping-Anfrage versendet. Ist diese erfolgreich, folgt ein UDP-Paket mit der Payload 0. Ist der Ping erfolglos oder der ICMP-Port nicht erreichbar, gilt die Verbindung als ausgefallen.

   Port (nur bei den Überwachungstypen *TCP* und *UDP*): Port-Nummer, an die die Anfrage gesendet wird.

   URL (optional, nur bei Überwachungstypen *HTTP/S Host*): Anzufragende URL.Sie können statt den Standard-Ports 80 und 443 auch andere Ports verwenden, indem Sie die Port-Information an die URL anhängen, z. B. `http://beispiel.domaene:8080/index.html`. Wenn keine URL angegeben ist, wird das Wurzelverzeichnis angefragt.

   Intervall: Geben Sie eine Zeitspanne in Sekunden an, in der die Hosts überprüft werden.

   Zeitüberschreitung: Geben Sie einen maximalen Zeitraum in Sekunden an, in dem die überwachenden Hosts eine Antwort senden können. Wenn keiner der

überwachenden Hosts einer Schnittstelle in diesem Zeitraum antwortet, wird die Schnittstelle als tot betrachtet.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Eine neue virtuelle Schnittstelle namens *Uplink Interfaces* wird automatisch angelegt und steht anderen Funktionen von Sophos UTM zur Verfügung, z. B. IPsec-Regeln. Die virtuelle Netzwerkschnittstelle *Uplink Interfaces* umfasst alle Uplink-Schnittstellen, die der Schnittstellen-Liste hinzugefügt wurden.
Eine neue virtuelle Schnittstelle namens *Uplink Primary Addresses* (Uplink-Hauptadressen) wird automatisch angelegt und steht anderen Funktionen von Sophos UTM zur Verfügung, z. B. Firewallregeln.Sie bezieht sich auf die Hauptadressen sämtlicher *Uplink-Schnittstellen*.

Im Fall des Versagens einer Schnittstelle können offene VPN-Tunnel automatisch über die nächste verfügbare Schnittstelle wiederhergestellt werden, vorausgesetzt, dass DynDNS verwendet wird oder der entfernte Server die IP-Adressen aller Uplink-Schnittstellen akzeptiert. Voraussetzung ist, dass die IPsec-Regel die *Uplink-Schnittstellen* als *Lokale Schnittstelle* verwendet.

6.1.5 Multipathregeln

Auf der Registerkarte *Schnittstellen & Routing* > *Schnittstellen* > *Multipathregeln* können Sie Regeln für den Uplink-Ausgleich erstellen. Die Regeln werden auf die aktiven Schnittstellen der Registerkarte *Uplink-Ausgleich* angewendet, falls es mehr als eine Schnittstelle gibt, um Verkehr auszugleichen. Ohne Multipathregeln werden die Dienste über die Quelle ausgeglichen, d. h., der gesamte von einer Quelle kommende Verkehr verwendet dieselbe Schnittstelle, während Verkehr von anderen Quellen zu anderen Schnittstellen geleitet werden kann. Mit Multipathregeln können Sie diese Standard-Schnittstellenbindung ändern.

Hinweis – Multipathregeln können für die Diensttypen TCP, UDP oder IP eingerichtet werden.

Um eine Multipathregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Multipathregeln* auf *Neue Multipathregel*.**
   Das Dialogfenster *Neue Multipathregel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Multipathregel ein.

Position: Die Positionsnummer legt die Priorität der Regel fest. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Sobald eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen. Platzieren Sie spezifischere Regeln oben in der Liste, um sicherzustellen, dass ungenauere Regeln zuletzt abgeglichen werden.

Quelle: Wählen Sie eine Quell-IP-Adresse oder ein Quellnetzwerk aus, auf die oder das die Regel sich beziehen soll.

Dienst: Wählen Sie einen Netzwerkdienst aus, auf den die Regel sich beziehen soll.

Ziel: Wählen Sie eine Ziel-IP-Adresse oder ein Quellnetzwerk aus, auf die oder das die Regel sich beziehen soll.

Tipp –Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

Schnittst.-Bindung: *Schnittstellen-Bindung* ist ein Verfahren, das gewährleistet, dass Datenverkehr mit bestimmten Attributen immer über dieselbe Uplink-Schnittstelle geroutet wird.Die Bindung hat eine Zeitbeschränkung von einer Stunde. Sie können diese Einstellung jedoch auf der Registerkarte *Uplink-Ausgleich* ändern. Sie können bestimmen, was die Basis für die Bindung sein soll:

- **Nach Verbindung:** Der (Standard-)Ausgleich erfolgt abhängig von der Verbindung, d. h. sämtlicher Datenverkehr, der zu einer bestimmten Verbindung gehört, verwendet dieselbe Schnittstelle, während Datenverkehr einer anderen Verbindung an eine andere Schnittstelle gesendet werden kann.
- **Nach Quelle:** Ausgleich erfolgt abhängig von der Quell-IP-Adresse, d. h. sämtlicher Datenverkehr, der aus einer Quelle stammt, verwendet dieselbe Schnittstelle, während Datenverkehr aus anderen Quellen an eine andere Schnittstelle gesendet werden kann.

  Hinweis – Die Bindung nach Quelle funktioniert nicht, wenn Sie einen Proxy verwenden, weil die Information über die ursprüngliche Quelle fehlt. Der HTTP-Proxy ist jedoch eine Ausnahme: Vom HTTP-Proxy generierter Verkehr stimmt mit der ursprünglichen Client-Quell-IP-Adresse überein und entspricht daher auch den Schnittstellenbindungsregeln *Nach Quelle*.

- **Nach Ziel:** Ausgleich erfolgt abhängig von der Ziel-IP-Adresse, d. h. sämtlicher Datenverkehr für ein Ziel verwendet dieselbe Schnittstelle, während Datenverkehr mit anderen Zielen an eine andere Schnittstelle gesendet werden kann.
- **Nach Quelle/Ziel:** Ausgleich erfolgt abhängig von Quell- und Ziel-IP-Adresse, d. h. sämtlicher Datenverkehr aus einer bestimmten Quelle und mit einem bestimmten Ziel verwendet dieselbe Schnittstelle. Datenverkehr mit einer anderen Kombination aus Quelle und Ziel kann an eine andere Schnittstelle gesendet werden. Beachten Sie bitte den obigen Hinweis.
- **Nach Schnittstelle:** Wählen Sie eine Schnittstelle aus der Auswahlliste *Bind-Schnittstelle*. Der Verkehr, für den diese Regel zutrifft, wird über diese Schnittstelle geroutet. Wenn eine Schnittstelle versagt und keine der folgenden Regeln zutrifft, wird für die Verbindung die Standardaktion angewendet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Ausgleich an (nicht mit Bindung nach Schnittstelle): Fügen Sie eine Schnittstellengruppe zum Feld hinzu. Der Verkehr, für den diese Regel zutrifft, wird über die Schnittstellen dieser Gruppe ausgeglichen. Standardeinstellung ist *Uplink-Schnittstellen*, d. h. Verbindungen werden über alle Uplink-Schnittstellen ausgeglichen.

   Regel bei Schnittstellenfehler überspringen: Ist die Option ausgewählt, wird im Fall eines Schnittstellenfehlers die nächste passende Multipathregel für den Verkehr verwendet. Ist die Option nicht ausgewählt, wird im Fall eines Schnittstellenfehlers keine andere Multipathregel auf den definierten Verkehr angewendet. Dies ist beispielsweise sinnvoll, wenn Sie sicherstellen möchten, dass SMTP-Verkehr nur von einer bestimmten statischen IP-Adresse gesendet wird, um zu verhindern, dass die Empfänger Ihre E-Mails aufgrund einer ungültigen Absender-IP-Adresse als Spam klassifizieren.
4. **Klicken Sie auf *Speichern*.**
   Die neue Multipathregel wird in der Liste *Multipathregeln* angezeigt.
5. **Aktivieren Sie die Multipathregel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

   Die Regel ist jetzt aktiv (Schieberegler ist grün).

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.1.6 Hardware

Auf der Registerkarte *Schnittstellen & Routing* > *Schnittstellen* > *Hardware* sind alle konfigurierten Schnittstellen mit den entsprechenden Hardware-Informationen wie z. B. dem Ethernet-Betriebsmodus und der MAC-Adresse aufgelistet. Bei UTM-Hardware-Geräten kann für jede Schnittstelle die automatische Aushandlung (Auto Negotiation) eingeschaltet oder ausgeschaltet werden.

Auto Negotiation (Automatische Aushandlung): Gewöhnlich wird der Ethernet-Betriebsmodus (1000BASE-T Full-Duplex, 100BASE-T Full-Duplex, 100BASE-T Half-Duplex, 10BASE-T Full-Duplex 10BASE-T Half-Duplex, usw.) zwischen zwei Netzwerkgeräten automatisch ausgehandelt, indem der beste Betriebsmodus gewählt wird, der von beiden Geräten unterstützt wird. Dabei wird eine höhere Geschwindigkeit (z. B. 1.000 Mbit/s) einer niedrigeren Geschwindigkeit (z. B. 100 Mbit/s) vorgezogen, bei gleicher Geschwindigkeit wird Full-Duplex Half-Duplex vorgezogen.

Warnung – Für eine einwandfreie Funktion von 1.000 Mbit/s ist die automatische Aushandlung stets erforderlich und wird auch vom IEEE-Standard 802.3ab gefordert. Achten Sie deshalb darauf, *Auto Negotiation* für Schnittstellen mit *Link mode 1000BASE-T* niemals auszuschalten. Die zeitliche Abstimmung Ihrer Netzwerkverbindung könnte scheitern, was zu eingeschränkter Funktionalität oder vollständigem Versagen führen kann. Bei der Verwendung von 100 Mbit/s und 10 Mbit/s ist die automatische Aushandlung optional, ihr Einsatz wird aber – sofern möglich – empfohlen.

Die automatische Aushandlung ist standardmäßig aktiviert. Klicken Sie in den seltenen Fällen, in denen sie abgeschaltet werden muss, auf die Schaltfläche *Bearbeiten* der entsprechenden Netzwerkkarte und ändern Sie die Einstellung in dem angezeigten Dialogfeld *NIC-Parameter bearbeiten* über die Auswahlliste *Link-Modus*. Beachten Sie, dass die Auswahlliste nur bei UTM-Hardware-Geräten verfügbar ist. Klicken Sie auf *Speichern*, um Ihre Änderungen zu speichern.

Warnung – Seien Sie vorsichtig, wenn Sie die automatische Aushandlung abschalten, da dadurch die Leistung der Verbindung deutlich eingeschränkt oder sogar unterbrochen werden kann. Falls es sich bei der Netzwerkkarte um Ihre Schnittstelle zum WebAdmin handelt, wäre in diesem Fall kein Zugriff auf den WebAdmin mehr möglich!

Im Fall, dass eine der Schnittstellen ihre Netzwerkverbindung aufgrund einer Änderung an der automatischen Aushandlung oder den Geschwindigkeitseinstellungen verloren hat, stellt eine Änderung der Einstellung auf ihren ursprünglichen Wert normalerweise die Funktionalität nicht wieder her: Das Ändern der automatischen Aushandlung oder der Geschwindigkeitseinstellungen von nicht verbundenen Schnittstellen funktioniert nicht zuverlässig. Aktivieren Sie daher erst die automatische Aushandlung und starten Sie dann UTM neu, um die normale Funktionalität wiederherzustellen.

HA-Link-Überwachung: Wenn Hochverfügbarkeit aktiviert ist, werden alle konfigurierten Schnittstellen auf ihren Link-Status hin überwacht. Falls ein Link ausfällt, wird eine Übernahme (Takeover) eingeleitet. Falls eine konfigurierte Schnittstelle nicht durchgehend verbunden ist (z. B. die Administrationsschnittstelle), deaktivieren Sie bitte die HA-Link-Überwachung für diese Schnittstelle. Andernfalls werden alle HA-Knoten im Status NICHT VERBUNDEN verbleiben. Um die HA-Link-Überwachung zu deaktivieren, klicken Sie auf die Schaltfläche *Bearbeiten* der entsprechenden Netzwerkkarte und ändern Sie die Einstellung im angezeigten Dialogfeld *NIC-Parameter bearbeiten*. Klicken Sie auf *Speichern*, um Ihre Änderungen zu speichern.

Virtuelle MAC setzen: Unter Umständen ist es sinnvoll, die MAC-Adresse eines Geräts zu ändern. Beispielsweise müssen die Modems einiger ISPs zurückgesetzt werden, wenn sich das angeschlossene Gerät und die damit verbundene MAC-Adresse ändert. Ein Zurücksetzen des Modems lässt sich vermeiden, indem die MAC-Adresse auf den Wert des Vorgängergeräts gesetzt wird.

UTMüberschreibt jedoch nicht die ursprüngliche MAC-Adresse des Geräts, sondern legt stattdessen eine virtuelle MAC-Adresse fest.Klicken Sie dazu auf die Schaltfläche *Bearbeiten* der entsprechenden Netzwerkkarte. Wählen Sie im angezeigten Dialogfeld *NIC-Parameter bearbeiten* die Option *Virtuelle MAC setzen* und geben Sie eine gültige MAC-Adresse ein.Klicken Sie auf *Speichern*, um Ihre Änderungen zu speichern.

Klicken Sie auf die Schaltfläche *Bearbeiten* der entsprechenden Netzwerkkarte, um die ursprüngliche MAC-Adresse wiederherzustellen. Wählen Sie im angezeigten Dialogfeld *NIC-Parameter bearbeiten* die Option *Virtuelle MAC setzen* ab.Klicken Sie auf *Speichern*, um Ihre Änderungen zu speichern.

6.2 Bridging

Das Bridging ist eine Methode zur Weiterleitung von Datenpaketen und wird hauptsächlich in Ethernet-Netzwerken eingesetzt. Im Gegensatz zum Routing trifft Bridging keine Annahmen

darüber, wo sich in einem Netzwerk eine bestimmte Adresse befindet. Stattdessen benutzt es Broadcasting, um unbekannte Geräte zu lokalisieren.

Durch Bridging können zwei oder auch mehrere gleichartige Netzwerke oder Netzwerksegmente miteinander verbunden werden. Dabei werden die Datenpakete mittels Bridging-Tabellen, die MAC-Adressen einem Bridge-Port zuordnen, weitergeleitet. Die entstehende Bridge übermittelt den Verkehr dann transparent durch die Bridging-Schnittstellen.

Hinweis – Diese Art von Verkehr muss explizit durch entsprechende Firewallregeln erlaubt werden.

Hinweis – Die meisten virtuellen Hosts lassen standardmäßig keine Änderungen von MAC-Adressen oder den Promiscuous Mode auf ihren virtuellen Schnittstellen zu. Damit Bridging auf virtuellen Hosts ausgeführt werden kann, stellen Sie sicher, dass die Validierung auf den MAC-Adressen des virtuellen Hosts deaktiviert und der Promiscuous Mode zugelassen ist.

6.2.1 Status

Um eine Bridge zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Bridging auf der Registerkarte *Status*.**
   Klicken Sie auf der Registerkarte *Schnittstellen & Routing* > *Bridging* > *Status* auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Bridge-Konfiguration* kann nun bearbeitet werden.

2. **Wählen Sie den Bridging-Modus aus.**
   Sie können zwischen zwei Bridging-Modi wählen:

   - **Bridge über alle NICs:** Bei dieser Methode werden alle verfügbaren Ethernet-Netzwerkkarten zu einer einzigen Bridge-Schnittstelle zusammengefasst. Die Festlegung einer *Konvertierungsschnittstelle* ist in diesem Modus Pflicht. Alle Schnittstellen außer der konvertierten Schnittstelle werden bei dieser Methode gelöscht.

   - **Bridge über ausgewählte NICs:** In diesem Modus können die NICs für die Bridge individuell zusammengestellt werden. Hierfür werden mindestens zwei unkonfigurierte Netzwerkkarten benötigt. Wählen Sie eine oder mehrere Netzwerkkarten aus, die Teil der Bridge werden sollen. Außerdem besteht die

Möglichkeit, eine *Konvertierungsschnittstelle* zu bestimmen, die auf die neue Bridge übertragen wird.

Hinweis – Zur Linkbündelung können Sie zwei LAG-Schnittstellen bridgen, z. B., indem Sie eine dieser Schnittstellen als *Konvertierungsschnittstelle* verwenden.

3. **Wählen Sie die Netzwerkkarte für die Bridge aus.**
   Für das Bridging kann nur eine bereits konfigurierte Netzwerkkarte ausgewählt werden. Die Bridge übernimmt die Adresseinstellungen dieser Schnittstelle sowie die Alias-Adressen und die VLAN-Einstellungen.

4. **Klicken Sie auf *Bridge einrichten*.**
   Die Netzwerkkarten werden nun zusammengefasst und die Bridge wird aktiviert (Schieberegler ist grün).

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

Sobald die Bridge konfiguriert ist, erscheint die umgewandelte Schnittstelle als Bridge-Gerät mit der SysID `br0` auf der Registerkarte *Schnittstellen & Routing* > *Schnittstellen*. Alle Schnittstellen, die zur Bridge gehören, werden in der *Bridge-Konfiguration* angezeigt. Um eine Schnittstelle aus der Bridge zu entfernen, wählen Sie die entsprechende Option ab und klicken Sie auf *Bridge aktualisieren*.

Um die Bridge zu entfernen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Status* auf den Schieberegler.**
   Der Schieberegler wird gelb.

2. **Klicken Sie auf *Entfernen der Bridge bestätigen*.**
   Der Schieberegler wird grau. Die Bridge wurde erfolgreich entfernt.

6.2.2 Erweitert

Auf der Registerkarte *Schnittstellen & Routing* > *Bridging* > *Erweitert* können die folgenden Optionen konfiguriert werden:

ARP-Broadcasts zulassen: Mit dieser Funktion können Sie bestimmen, ob eingehende ARP-Broadcasts von der Bridge weitergeleitet werden sollen. Im eingeschalteten Zustand erlaubt die Bridge Anfragen an die MAC-Zieladresse `FF:FF:FF:FF:FF:FF`. Dies kann eventuell von mutmaßlichen Angreifern genutzt werden, um Informationen über die Netzwerkkarten im entsprechenden Netzwerksegment oder sogar auf dem Gerät selbst zu

sammeln. Daher ist die Standardeinstellung, solche Broadcasts nicht durch die Bridge zu lassen.

Spanning Tree Protocol: Wenn diese Option aktiviert ist, wird das Spanning Tree Protocol (STP) aktiviert. Dieses Netzwerkprotokoll erkennt und verhindert Bridge-Loops.

Achtung – Beachten Sie, dass das Spanning Tree Protocol keinen Schutz bietet. Daher können Angreifer möglicherweise die Bridge-Topologie ändern.

Ablaufzeit: In diesem Eingabefeld stellen Sie ein, nach welcher Zeitspanne eine inaktive MAC-Adresse gelöscht wird. Standardmäßig ist als Zeitraum 300 Sekunden voreingestellt.

IPv6-Durchleitung zulassen: Aktivieren Sie diese Option, um die Durchleitung von IPv6-Verkehr über die Bridge ohne Kontrolle zuzulassen.

Virtuelle MAC-Adresse: Hier können Sie eine statische MAC-Adresse für die Bridge eingeben. Standardmäßig (und solange der Eintrag 00:00:00:00:00:00 lautet) verwendet die Bridge die niedrigste MAC-Adresse aller zugehörigen Schnittstellen.

Weitergeleitete EtherTypes: Standardmäßig leitet eine Bridge, die auf Sophos UTM konfiguriert ist, nur IP-Pakete weiter. Wenn Sie möchten, dass weitere Protokolle weitergeleitet werden, müssen Sie deren EtherType in dieses Feld eingeben. Die Typen müssen als 4-stellige hexadezimale Zahlen angegeben werden. Beliebte Beispiele sind AppleTalk (Typ 809B), Novell (Typ 8138) oder PPPoE (Typen 8863 und 8864). Ein typischer Fall wäre eine Bridge zwischen Ihren RED-Schnittstellen, die zusätzliche Protokolle zwischen den verbundenen Netzwerken weiterleiten sollen.

6.3 Dienstqualität (QoS)

Im Allgemeinen bezeichnet *Dienstqualität* (QoS, Quality of Service) Kontrollmechanismen, die dafür sorgen, dass ausgewählter Netzwerkverkehr bevorzugt behandelt und insbesondere dass diesem eine Mindestbandbreite zugesichert wird. In Sophos UTM wird zu priorisierender Verkehr auf der Registerkarte *Dienstqualität (QoS)* konfiguriert. Hier können Sie für bestimmte Arten von ausgehendem Verkehr, der zwei Punkte im Netzwerk passiert, eine garantierte Bandbreite reservieren. Dahingegen wird die Optimierung von Kapazitäten (engl. traffic shaping) für eingehenden Verkehr intern durch verschiedene Techniken umgesetzt, z. B. durch *Stochastic Fairness Queuing* (SFQ) oder *Random Early Detection* (RED).

6.3.1 Status

Auf der Registerkarte *Dienstqualität (QoS) > Status* sind die Netzwerkkarten aufgelistet, für die QoS konfiguriert werden kann. Standardmäßig ist QoS für alle Schnittstellen ausgeschaltet.

Um QoS für eine Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Bearbeiten* der entsprechenden Schnittstelle.**
   Das Dialogfeld *Schnittstelle bearbeiten* öffnet sich.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Downlink Kbit/s/Uplink Kbit/s: Geben Sie die Bandbreiten, die Ihr ISP bereitstellt, für Uplink und Downlink (in Kbit/s) ein. Um beispielsweise eine Internetverbindung mit 5 Mbit/s für Up- und Downlink zu konfigurieren, geben Sie `5120` ein.

   Sollte Ihre Bandbreite variieren, geben Sie den niedrigsten garantierten Wert an, der von Ihrem ISP zugesichert wird. Wenn Sie beispielsweise eine Internetverbindung mit 5 Mbit/s für Up- und Downlink mit einer Variation von 0,8 Mbit/s haben, geben Sie 4300 Kbit/s an. Beachten Sie, dass das Gateway eine veränderte Bandbreite berücksichtigt, wenn die verfügbare Bandbreite temporär höher ausfällt als der konfigurierte tiefste zugesicherte Wert. Dabei wird der prozentuale Anteil an der Bandbreite für zu priorisierenden Verkehr entsprechend erhöht; umgekehrt funktioniert das jedoch leider nicht.

   Uplink begrenzen: Wenn Sie diese Option wählen, nutzt die Funktion QoS die oben eingetragenen Bandbreitenwerte als Basis für die Kalkulation des zu priorisierenden Datenverkehrs, der diese Schnittstelle passiert. Die Option *Uplink begrenzen* ist standardmäßig ausgewählt und sollte für die folgenden Arten von Schnittstellen verwendet werden:

   - Ethernet-Statisch-Schnittstelle: Zwischen Gateway und Internet ist ein Router installiert und die vom Router bereitgestellte Bandbreite ist bekannt.
   - Ethernet-VLAN-Schnittstelle: Zwischen Gateway und Internet ist ein Router installiert und die vom Router bereitgestellte Bandbreite ist bekannt.
   - DSL (PPPoE)
   - DSL (PPPoA)
   - Modem (PPP)

Die Option *Uplink begrenzen* sollte grundsätzlich für jene Schnittstellen ausgeschaltet werden, bei denen die Basis für die Bandbreiten-Kalkulation schon durch die Maximalgeschwindigkeit der jeweiligen Schnittstelle ermittelt werden kann. Dies betrifft jedoch nur die folgenden Schnittstellen-Typen:

- Ethernet-Statisch-Schnittstelle: Direkt mit dem Internet verbunden.
- Ethernet-VLAN-Schnittstelle: Direkt mit dem Internet verbunden.
- Ethernet-DHCP

Bei Schnittstellen ohne eine Uplink-Grenze verteilt die QoS-Funktion den gesamten Datenverkehr proportional. Wenn Sie beispielsweise auf einer Ethernet-DHCP-Schnittstelle 512 Kbit/s für VoIP-Verkehr reserviert haben und sich die verfügbare Bandbreite halbiert, dann würden 256 Kbit/s für diesen Datenverkehr verwendet werden (im Gegensatz zu Schnittstellen mit einer festen Obergrenze funktioniert proportionale Verteilung in beiden Richtungen).

Download-Ausgleich: Wenn diese Option aktiviert ist, verhindern die beiden Warteschlangen-Algorithmen *Stochastic Fairness Queuing* (SFQ) und *Random Early Detection* (RED), dass es zu Netzwerkstaus kommt. Im Fall dass die konfigurierte Download-Geschwindigkeit erreicht ist, werden Pakete jener Verbindung verworfen, die den meisten Downlink in Anspruch nimmt.

Upload-Optimierung: Wenn diese Option aktiviert ist, werden ausgehende TCP-Pakete, die eine Verbindung aufbauen, priorisiert (TCP-Pakete mit *SYN*-Flag) ebenso wie TCP-Bestätigungspakete (TCP-Pakete mit *ACK*-Flag und einer Paketlänge zwischen 40 und 60 Byte) und DNS-Lookups (UDP-Pakete auf Port `53`).

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

4. **Aktivieren Sie QoS für die Schnittstelle.**
   Klicken Sie auf den Schieberegler der Schnittstelle. Der Schieberegler wird grün.

6.3.2 Verkehrskennzeichner

Ein Verkehrskennzeichner (traffic selector) kann als eine QoS-Definition angesehen werden, die bestimmte Arten von Netzwerkverkehr beschreibt, die von QoS bearbeitet werden. Diese Definitionen werden später innerhalb der Bandbreiten-Pool-Definition verwendet. Dort können Sie festlegen, wie dieser Verkehr von QoS behandelt wird, indem Sie z. B. die komplette Bandbreite begrenzen oder dem Verkehr einen gewissen Mindestanteil der Bandbreite zusichern.

Um einen Verkehrskennzeichner anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verkehrskennzeichner* auf *Neuer Verkehrskennzeichner*.**
   Das Dialogfeld *Neuen Verkehrskennzeichner erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diesen Verkehrskennzeichner ein.

   Kennzeichnertyp: Sie können folgende Arten von Kennzeichnern festlegen:

   - **Verkehrskennzeichner:** Verwenden Sie einen Verkehrskennzeichner, wird der Verkehr auf Grundlage eines einzelnen Dienstes oder einer Dienstgruppe reguliert.
   - **Anwendungskennzeichner:** Verwenden Sie einen Anwendungskennzeichner, wird der Verkehr auf Grundlage von Anwendungen reguliert, d. h. je nachdem, zu welcher Anwendung er gehört, unabhängig vom verwendeten Port oder Dienst.
   - **Gruppe:** Sie können verschiedene Dienst- und Anwendungskennzeichner in einer Verkehrskennzeichnerregel zusammenfassen. Um eine Gruppe definieren zu können, müssen bereits einzelne Kennzeichner definiert sein.

   Quelle: Fügen Sie das Quellnetzwerk hinzu oder wählen Sie das Quellnetzwerk aus, für das QoS aktiviert werden soll.

   Dienst: Nur für *Verkehrskennzeichner*. Fügen Sie den Netzwerkdienst hinzu oder wählen Sie den Netzwerkdienst aus, für den QoS aktiviert werden soll. Sie können zwischen verschiedenen vordefinierten Diensten und Dienstgruppen auswählen. Wenn Sie beispielsweise für VoIP-Verbindungen eine bestimmte Bandbreite reservieren möchten, wählen Sie VoIP-Protokolle (SIP und H.323) aus.

   Ziel: Fügen Sie das Zielnetzwerk hinzu oder wählen Sie das Zielnetzwerk aus, für das QoS aktiviert werden soll.

   Tipp – Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Kontrollieren durch: Nur für *Anwendungskennzeichner*. Wählen Sie aus, ob die Regulierung des Verkehrs auf Grundlage des jeweiligen Anwendungstyps oder kategoriebasiert durch einen dynamischen Filter erfolgen soll.

- **Anwendungen:** Der Verkehr wird anwendungsbasiert reguliert. Wählen Sie im Feld *Diese Anwendungen kontrollieren* eine oder mehrere Anwendungen aus.
- **Dynamischer Filter:** Der Verkehr wird kategoriebasiert reguliert. Wählen Sie im Feld *Diese Kategorien kontrollieren* eine oder mehrere Kategorien aus.

Diese Anwendungen/Kategorien kontrollieren: Nur für *Anwendungskennzeichner*. Klicken Sie auf das Ordnersymbol, um Anwendungen/Kategorien auszuwählen. Ein Dialogfenster wird geöffnet, das im nächsten Abschnitt detailliert beschrieben wird.

Produktivität: Nur mit *Dynamischer Filter*. Gibt den von Ihnen gewählten Produktivitätswert wieder.

Risiko: Nur mit *Dynamischer Filter*. Gibt den von Ihnen gewählten Risikowert wieder.

Hinweis – Einige Anwendungen sind von der Regulierung ausgeschlossen. Dies ist für einen reibungslosen Betrieb von Sophos UTM erforderlich. Bei diesen Anwendungen wird in der Anwendungstabelle des Dialogfensters *Anwendung auswählen* kein Auswahlkästchen angezeigt. Dies trifft u. a. für den *WebAdmin*, *Teredo*, *SixXs* (für IPv6-Verkehr) und *Portal* (für Benutzerportal-Verkehr) zu. Wenn Sie dynamische Filter verwenden, wird die Regulierung dieser Anwendungen ebenfalls automatisch verhindert.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**

TOS/DSCP (nur beim Kennzeichnertyp *Verkehrskennzeichner*): In bestimmten Fällen kann es sinnvoll sein, Datenverkehr, der von QoS bearbeitet werden soll, nicht nur über Quelle, Ziel und Dienst zu unterscheiden, sondern auch über die TOS- oder DSCP-Flags im IP-Header.

- **Aus:** Mit dieser Standardoption wird sämtlicher Datenverkehr, der mit Quelle, Dienst und Ziel übereinstimmt, der oben eingestellt wurde, mit QoS bearbeitet.
- **TOS-Bit:** Wählen Sie diese Option aus, wenn der mit QoS bearbeiteten Datenverkehr auf IP-Pakete mit bestimmten TOS-Bit (Type of Service) beschränkt werden soll. Sie können zwischen den folgenden Einstellungen wählen:

   - Normaler Dienst
   - Kosten minimieren
   - Zuverlässigkeit maximieren
   - Durchsatz maximieren
   - Verzögerung minimieren

- **DSCP-Bit:** Wählen Sie diese Option aus, wenn der mit QoS bearbeiteten Datenverkehr auf IP-Pakete mit bestimmten DSCP-Bit (Differentiated Services Code Point) beschränkt werden soll. Sie können entweder einen einzigen *DSCP-Wert* festlegen (eine Ganzzahl im Bereich 0 bis 63) oder einen vordefinierten Wert aus der Liste *DSCP-Klassen* (z. B. *BE default dscp (000000)*) auswählen.

Datenmenge gesendet/empfangen: Aktivieren Sie dieses Auswahlkästchen, wenn der Verkehrskennzeichner die Übereinstimmung aufgrund der Anzahl der von der Verbindung bisher übertragenen Byte vornehmen soll. Mit dieser Funktion können Sie beispielsweise die Bandbreite von großen HTTP-Uploads einschränken, ohne den normalen HTTP-Verkehr zu beeinträchtigen.

- **Gesendet/empfangen:** Wählen Sie aus der Auswahlliste *Mehr als* aus, um den Verkehrskennzeichner nur für Verbindungen zu definieren, die eine bestimmte Verkehrsmenge überschreiten. Wählen Sie *Weniger als* aus, um ihn für Verbindungen mit bisher weniger Verkehr zu definieren.
- **kByte:** Geben Sie den Schwellenwert für die Verkehrsmenge ein.

Helfer: Einige Dienste nutzen für die Datenübertragung dynamische Ports. Für jede Verbindung verhandeln die Endpoints die zu verwendenden Ports über einen Kontrollkanal. Die UTM verwendet einen speziellen Helfer für die Verbindungsverfolgung (engl. connection tracking helper), der den Kontrollkanal überwacht, um herauszufinden, welche dynamischen Ports verwendet werden. Um den Verkehr, der durch die dynamischen Ports geht, in den Verkehrskennzeichner mit aufzunehmen, wählen Sie oben, im Feld *Dienst*, *Any*, und wählen Sie in der Auswahlliste *Helfer* den entsprechenden Dienst.

4. **Klicken Sie auf *Speichern*.**
   Der neue Kennzeichner wird in der Liste *Verkehrskennzeichner* angezeigt.

Wenn Sie viele Verkehrskennzeichner definiert haben, können Sie mehrere Kennzeichner zu einer Verkehrskennzeichnergruppe zusammenfügen, um die Konfiguration bequemer zu gestalten.

Dieser Verkehrskennzeichner oder diese Verkehrskennzeichnergruppe kann nun für jeden Bandbreiten-Pool verwendet werden. Diese Pools können auf der Registerkarte *Bandbreiten-Pools* definiert werden.

Das Dialogfenster zur Auswahl von Anwendungen oder Kategorien

Beim Erstellen von Application-Control-Regeln müssen Sie Anwendungen oder Anwendungskategorien aus dem Dialogfenster *Wählen Sie eine oder mehrere Anwendungen/Kategorien, die kontrolliert werden sollen* festlegen.

In der Tabelle im unteren Bereich des Dialogfensters werden die Anwendungen angezeigt, die auswählbar sind oder zu einer definierten Kategorie gehören. Standardmäßig werden alle Anwendungen angezeigt.

Im oberen Bereich des Dialogfensters stehen drei Konfigurationsoptionen zur Wahl, mit deren Hilfe die Anzahl der in der Tabelle gelisteten Anwendungen eingeschränkt werden kann:

- **Kategorie:** Die Anwendungen werden nach Kategorie gruppiert. Diese Liste umfasst alle verfügbaren Kategorien. Standardmäßig sind alle Kategorien ausgewählt; d. h. alle verfügbaren Anwendungen werden unten in der Tabelle gelistet. Möchten Sie die angezeigten Anwendungen auf bestimmte Kategorien beschränken, klicken Sie in die Liste mit den Kategorien und wählen Sie nur die gewünschte(n) Kategorie(n) aus.
- **Produktivität:** Die Anwendungen werden zudem nach ihrer Auswirkung auf die Produktivität klassifiziert, d. h., wie stark sie die Produktivität beeinflussen. Beispiel: Salesforce, eine typische Unternehmenssoftware, besitzt die Bewertung 5. Die Nutzung der Anwendung trägt somit zur Produktivität bei. Im Gegensatz dazu ist das Onlinespiel Farmville mit 1 bewertet und dadurch kontraproduktiv. Der Netzwerkdienst DNS besitzt die Bewertung 3 – er wirkt sich neutral auf die Produktivität aus.
- **Risiko:** Anwendungen werden auch hinsichtlich ihres Risikos bezüglich Schadsoftware, Virusinfektionen oder Angriffen klassifiziert. Je höher die Bewertung, desto höher das Risiko.

Tipp – Jede Anwendung verfügt über ein Infosymbol. Wenn Sie darauf klicken, wird eine Beschreibung der jeweiligen Anwendung angezeigt. Sie können die Tabelle mit Hilfe des Filterfelds in der Kopfzeile durchsuchen.

Abhängig von Ihrer Auswahl in der Auswahlliste „Kontrollieren durch“ im Dialogfeld *Neuen Verkehrskennzeichner erstellen* gehen Sie folgendermaßen vor:

- Kontrolle durch dynamischen Filter: Wählen Sie im Feld *Kategorie* die Kategorien aus und klicken Sie auf *Übernehmen*, um die ausgewählten Kategorien für die Regel zu übernehmen.
- Anwendungsbasierte Kontrolle: Wählen Sie die zu kontrollierenden Anwendungen in der Tabelle aus, indem Sie auf die Auswahlkästchen klicken, die vor den Anwendungen angezeigt werden. Klicken Sie auf *Übernehmen*, um die ausgewählten Anwendungen für die Regel zu übernehmen.

Nachdem Sie auf *Übernehmen* geklickt haben, wird das Dialogfenster geschlossen und Sie können die Einstellungen der Verkehrskennzeichnerregel weiter bearbeiten.

6.3.3 Bandbreiten-Pools

Auf der Registerkarte *Dienstqualität (QoS) > Bandbreiten-Pools* werden die Pools für das Bandbreiten-Management definiert und verwaltet. Mit einem Bandbreiten-Pool reservieren Sie eine garantierte Bandbreite für einen spezifischen ausgehenden Verkehrstyp, optional limitiert durch eine maximale Bandbreite.

Um einen Bandbreiten-Pool anzulegen, gehen Sie folgendermaßen vor:

1. **Wählen Sie auf der Registerkarte *Bandbreiten-Pools* eine Schnittstelle aus.**
   Wählen Sie aus der Auswahlliste *An Schnittstelle gebunden* diejenige Schnittstelle aus, für die Sie einen Bandbreiten-Pool definieren möchten.
2. **Klicken Sie auf *Neuer Bandbreiten-Pool*.**
   Das Dialogfeld *Neuen Bandbreiten-Pool erstellen* wird geöffnet.
3. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den Bandbreiten-Pool ein.

   Position: Die Positionsnummer legt die Priorität des Bandbreiten-Pools fest. Niedrigere Nummern haben eine höhere Priorität. Bandbreiten-Pools werden in aufsteigender Reihenfolge abgeglichen. Sobald ein Bandbreiten-Pool zutrifft, werden Bandbreiten-Pools mit einer höheren Nummer nicht mehr abgeglichen. Platzieren Sie spezifischere Pools oben in der Liste, um sicherzustellen, dass ungenauere Pools zuletzt abgeglichen werden. Beispiel: Sie haben einen Bandbreiten-Pool für Internet-Datenverkehr (HTTP) im Allgemeinen und einen weiteren Pool für den Internet-Datenverkehr zu einem bestimmten Webserver definiert. Dann sollte der Bandbreiten-Pool mit dem spezifischen Webserver vorrangig positioniert, d. h. auf Position 1 gesetzt werden.

Bandbreite: Tragen Sie die Uplink-Bandbreite (in Kbit) ein, die für diesen Bandbreiten-Pool reserviert werden soll.Wenn Sie z. B. 1 Mbit/s für eine bestimmte Art von Datenverkehr reservieren möchten, geben Sie `1024` ein.

> **Hinweis –** Sie können für einen Bandbreiten-Pool lediglich bis zu 90 % der zur Verfügung stehenden Gesamtbandbreite reservieren. Das Gateway reserviert grundsätzlich 10 % für den vom Bandbreiten-Management unberücksichtigten Datenverkehr. Um bei dem Beispiel von oben zu bleiben: Wenn der Uplink 5 Mbit/s beträgt, und Sie möchten VoIP soviel Bandbreite wie möglich zuweisen, können Sie für den VoIP-Datenverkehr eine Bandbreite von maximal 4608 Kbit/s reservieren.

Obere Bandbreitengrenze angeben: Der Wert, den Sie oben im Feld *Bandbreite* angegeben haben, stellt die zugesicherte Bandbreite dar, die für einen speziellen Verkehrstyp reserviert ist. Ein Bandbreiten-Pool beansprucht jedoch immer mehr Bandbreite für seinen Verkehr als verfügbar ist. Wenn Sie für einen bestimmten Verkehrstyp verhindern wollen, dass er mehr als eine bestimmte Menge Ihrer Bandbreite verbraucht, wählen Sie diese Option aus, um die Bandbreitennutzung dieses Pools auf eine Obergrenze zu beschränken.

Verkehrskennzeichner: Wählen Sie die Verkehrskennzeichner für diesen Bandbreiten-Pool aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

4. **Klicken Sie auf *Speichern*.**
   Der neue Bandbreiten-Pool wird in der Liste *Bandbreiten-Pools* angezeigt.

5. **Aktivieren Sie die Regel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

   Die Regel ist jetzt aktiv (Schieberegler ist grün).

Um einen Bandbreiten-Pool zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.3.4 Download-Drosselung

Auf der Registerkarte *Dienstqualität (QoS) > Download-Drosselung* können Sie Regeln definieren und verwalten, um eingehenden Verkehr zu drosseln. Wenn Pakete schneller ankommen als der eingestellte Schwellenwert, werden die überzähligen Pakete sofort verworfen, ohne im Firewall-Protokoll aufgelistet zu werden. Aufgrund von Mechanismen zur TCP-Überlastvermeidung (TCP congestion avoidance) sollten die betroffenen Absender als Reaktion auf die verworfenen Pakete ihre Senderaten reduzieren.

Um eine Download-Drosselungsregel zu erstellen, gehen Sie folgendermaßen vor:

1. **Wählen Sie auf der Registerkarte *Download-Drosselung* eine Schnittstelle.**
   Wählen Sie aus der Auswahlliste *An Schnittstelle gebunden* diejenige Schnittstelle aus, für die Sie eine Download-Drosselungsregel definieren möchten.

2. **Klicken Sie auf *Neue Download-Drosselungsregel*.**
   Das Dialogfeld *Neue Download-Drosselungsregel anlegen* wird geöffnet.

3. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Download-Drosselungsregel ein.

   Position: Die Positionsnummer legt die Priorität der Regel fest. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Sobald eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen.Platzieren Sie spezifischere Regeln oben in der Liste, um sicherzustellen, dass ungenauere Regeln zuletzt abgeglichen werden.

   Begrenzung (Kbit/s): Der obere Grenzwert (in Kbit) für den festgelegten Verkehr. Wenn Sie beispielsweise die Rate für einen bestimmten Verkehrstyp auf 1 Mbit/s begrenzen wollen, geben Sie 1024 ein.

   Limitiere: Kombination aus Verkehrsquelle und -ziel, auf die das oben definierte Limit zutreffen soll:

   - **verteilt:** Das Limit wird zwischen allen existierenden Verbindungen gleich verteilt. Die Gesamt-Downloadrate für den Verkehr, der durch diese Regel definiert ist, ist also auf den festgelegten Wert begrenzt.
   - **jede Quelladresse:** Das Limit wird auf jede einzelne Quelladresse angewendet.
   - **jede Zieladresse:** Das Limit wird auf jede einzelne Zieladresse angewendet.

- **jede Quelle-Ziel-Kombination:** Das Limit wird auf jedes einzelne Quelle-Ziel-Adresspaar angewendet.

  Verkehrskennzeichner: Wählen Sie die Verkehrskennzeichner, für die Sie die Downloadraten drosseln möchten. Das definierte Limit wird auf die gewählten Verkehrskennzeichner aufgeteilt.

  Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

4. **Klicken Sie auf *Speichern*.**
   Die neue Download-Drosselungsregel wird in der Liste *Download-Drosselung* angezeigt.

5. **Aktivieren Sie die Regel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

   Die Regel ist jetzt aktiv (Schieberegler ist grün).

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.3.5 Erweitert

Klassifizierung nach Verkapselung beibehalten

Markieren Sie dieses Auswahlkästchen, wenn Sie gewährleisten möchten, dass ein Paket nach der Verkapselung weiterhin dem Verkehrskennzeichner des ursprünglichen Dienstes zugewiesen wird, wenn es keinen anderen übereinstimmenden Verkehrskennzeichner gibt.

Die Zuweisung eines gekapselten IP-Pakets zu einem Verkehrskennzeichner erfolgt wie folgt:

1. Das ursprüngliche IP-Paket wird in der vorgegebenen Reihenfolge mit den vorhandenen Verkehrskennzeichnern abgeglichen. Das Paket wird dem ersten übereinstimmenden Verkehrskennzeichner zugewiesen (z. B. Internal -> HTTP -> Any).

2. Das IP-Paket wird gekapselt und der Dienst geändert (z. B. in IPsec).

3. Das gekapselte IP-Paket wird in der vorgegebenen Reihenfolge mit den vorhandenen Verkehrskennzeichnern abgeglichen. Das Paket wird dem ersten übereinstimmenden Verkehrskennzeichner zugewiesen (z. B. Internal -> IPsec -> Any).

4. Wenn kein Verkehrskennzeichner übereinstimmt, ist die Zuweisung von der Option *Klassifizierung nach Verkapselung beibehalten* abhängig:

- Ist die Option ausgewählt, wird das gekapselte Paket dem Verkehrskennzeichner aus Schritt 1 zugewiesen.
- Ist die Option nicht ausgewählt, wird das gekapselte Paket keinem Verkehrskennzeichner zugewiesen und kann daher nicht Bestandteil eines Bandbreiten-Pools sein.

Explicit-Congestion-Notification-Unterstützung

ECN (Explicit Congestion Notification) ist eine Erweiterung des Internetprotokolls und ermöglicht End-to-End-Benachrichtigungen über Netzwerküberlastungen, ohne dass Pakete verworfen werden. ECN funktioniert nur, wenn beide Endpoints einer Verbindung erfolgreich über die Verwendung verhandeln. Durch Markieren dieses Auswahlkästchens sendet die UTM die Information, dass sie bereit ist, ECN zu verwenden. Stimmt der andere Endpunkt zu, werden ECN-Informationen ausgetauscht. Beachten Sie, dass auch das zugrunde liegende Netzwerk und die beteiligten Router ECN unterstützen müssen.

6.4 Uplink-Überwachung

Das Menü *Schnittstellen & Routing > Uplink-Überwachung* gibt Ihnen die Möglichkeit, Ihre Uplink-Verbindung (Internet-Verbindung) zu überwachen und bestimmte Aktionen vorzugeben, die im Fall, dass sich der Verbindungsstatus ändert, automatisch ausgeführt werden.

Beispielsweise kann automatisch ein Ersatz-VPN-Tunnel aktiviert werden, der eine andere Verbindung benutzt. Oder es wird eine Alias-IP-Adresse deaktiviert, so dass ein Überwachungsdienst aktiviert wird.

6.4.1 Allgemein

Auf der Registerkarte *Uplink-Überwachung > Allgemein* können Sie die Uplink-Überwachung ein- oder ausschalten.

Um Uplink-Überwachung zu aktivieren, klicken Sie auf den Schieberegler.
Der Schieberegler wird grün.

Wenn die Uplink-Überwachung aktiv ist, zeigt der Bereich *Uplink-Status* alle aktuellen Uplink-Schnittstellen und deren Status an:

- *ONLINE:* Die Uplink-Verbindung ist hergestellt und funktioniert.
- *OFFLINE:* Die Überwachung hat festgestellt, dass die Uplink-Verbindung nicht funktioniert.
- *DOWN:* Entweder wurde die Uplink-Schnittstelle administrativ deaktiviert, oder – im Fall einer dynamischen Schnittstelle – der entfernte PPP- oder DHCP-Server ist nicht erreichbar.
- *STANDBY:* Die Schnittstelle wurde auf der Registerkarte *Schnittstellen* > *Uplink-Ausgleich* als Standby-Schnittstelle definiert und wird derzeit nicht verwendet.

Hinweis – Wenn der Uplink-Ausgleich aktiv ist, werden die Uplinks immer überwacht, selbst wenn Uplink-Überwachung deaktiviert ist. Daher werden, selbst wenn die Uplink-Überwachung ausgeschaltet ist, die Uplink-Schnittstellen auf dieser Seite angezeigt, wenn der Uplink-Ausgleich aktiv ist. In diesem Fall können Sie die Überwachungseinstellungen auf der Registerkarte *Schnittstellen* > *Uplink-Ausgleich* ändern.

6.4.2 Aktionen

Auf der Registerkarte *Schnittstellen & Routing* > *Uplink-Überwachung* > *Aktionen* können Sie Aktionen definieren, die im Fall, dass sich der Uplink-Status ändert, automatisch durchgeführt werden. Beispielsweise möchten Sie vielleicht zusätzliche Adressen deaktivieren, wenn die Uplink-Verbindung unterbrochen ist.

Um eine neue Aktion anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Aktionen* auf *Neue Aktion*.**
   Das Dialogfeld *Aktion 'falls Uplink offline geht' anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Aktion ein.

   Art: Wählen Sie den Verbindungstyp, für den Sie eine Aktion definieren wollen.

   - **IPsec-Tunnel:** Wählen Sie diese Option aus der Auswahlliste, wenn Sie eine Aktion für einen IPsec-Tunnel definieren wollen.
   - **Zusätzliche Adresse:** Wählen Sie diese Option aus der Auswahlliste, wenn Sie eine Aktion für eine zusätzliche Adresse definieren wollen.

IPsec-Tunnel: (Nur verfügbar wenn *IPsec-Tunnel* als Typ festgelegt wurde.) Wenn mindestens ein IPsec-Tunnel definiert ist, können Sie hier einen von ihnen auswählen. Weitere Informationen über IPsec-Tunnel finden Sie in Kapitel *Fernzugriff* > *IPsec*.

Zus. Adresse: (Nur verfügbar wenn *Zusätzliche Adresse* als Typ festgelegt wurde.) Wenn mindestens eine zusätzliche Adresse definiert ist, können Sie hier eine von ihnen auswählen. Weitere Informationen über zusätzliche Adressen finden Sie in Kapitel *Schnittstellen & Routing* > *Schnittstellen* > *Zusätzliche Adressen*.

Aktion: Sie können hier entweder *Enable* oder *Disable* wählen, was bedeutet, dass im Fall einer Uplink-Unterbrechung der oben gewählte IPsec-Tunnel oder die zusätzliche Adresse aktiviert oder deaktiviert wird.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die Aktion wird gespeichert und im Fall, dass die Uplink-Verbindung unterbrochen wird, ausgeführt.

Um eine Aktion zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.4.3 Erweitert

Auf der Registerkarte *Uplink-Überwachung* > *Erweitert* können Sie die automatische Überwachung der Uplink-Verbindung deaktivieren und stattdessen einen oder mehrere Hosts angeben, die für die Überwachung verwendet werden sollen.

Automatische Überwachung ist standardmäßig aktiviert, um ein mögliches Versagen einer Schnittstelle zu entdecken. Dies bedeutet, dass der Zustand aller Uplink-Schnittstellen überwacht wird, indem ein bestimmter Host im Internet in einem Abstand von 15 Sekunden angesprochen wird. Standardmäßig ist der überwachende Host der dritte Pings zulassende Hop auf dem Weg zu einem der Root-DNS-Server. Sie können die Hosts zum Überwachen der Server auch selbst bestimmen. Für diese Hosts können Sie einen anderen Dienst als Ping auswählen und Überwachungsintervall und -zeitüberschreitung anpassen:

Die überwachenden Hosts werden dann in gewissen Abständen angesprochen, und wenn keiner von ihnen erreichbar ist, gilt die Uplink-Verbindung als unterbrochen.Anschließend werden die Aktionen ausgeführt, die in der Registerkarte *Aktionen* definiert sind.

Hinweis – Automatisch werden dieselben Überwachungseinstellungen sowohl für die Uplink-Überwachung (*Uplink-Überwachung* > *Erweitert*) als auch für den Uplink-Ausgleich (*Schnittstellen* > *Uplink-Ausgleich*) verwendet.

Um Ihre eigenen Hosts für die Überwachung zu verwenden, gehen Sie folgendermaßen vor:

1. **Deaktivieren Sie das Auswahlkästchen *Automatische Überwachung*.**
   Das Feld *Überwachende Hosts* kann nun bearbeitet werden.

2. **Fügen Sie die überwachenden Hosts hinzu.**
   Wählen Sie einen oder mehrere Hosts aus oder fügen Sie Hosts hinzu, die anstelle einer zufälligen Auswahl an Hosts die Überwachung übernehmen sollen. Wenn eine Schnittstelle von mehr als einem Host überwacht wird, wird sie nur als tot betrachtet, wenn keiner der überwachenden Hosts in der festgelegten Zeitspanne antwortet. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   Hinweis – Wenn ein ausgewählter Host an eine Schnittstelle gebunden ist, wird er nur zur Überwachung dieser Schnittstelle verwendet. Ist ein Host nicht an eine Schnittstelle gebunden, wird er zur Überwachung aller Schnittstellen verwendet. Schnittstellen, die nicht von den ausgewählten Hosts überwacht werden, werden automatisch überwacht.

   Klicken Sie auf das Symbol Überwachungseinstellungen bearbeiten im Kopf des Feldes, um die Überwachungsdetails festzulegen:

   Überwachungstyp: Wählen Sie das Dienstprotokoll für die Überwachungsprüfungen aus. Wählen Sie für die Dienstüberwachung entweder *TCP* (TCP-Verbindungsaufbau), *UDP* (UDP-Verbindungsaufbau), *Ping* (ICMP-Ping), *HTTP Host* (HTTP-Anfragen) oder *HTTPS Host* (HTTPS-Anfragen). Wenn Sie *UDP* verwenden, wird zunächst eine Ping-Anfrage versendet. Ist diese erfolgreich, folgt ein UDP-Paket mit der Payload 0. Ist der Ping erfolglos oder der ICMP-Port nicht erreichbar, gilt die Verbindung als ausgefallen.

   Port (nur bei den Überwachungstypen *TCP* und *UDP*): Port-Nummer, an die die Anfrage gesendet wird.

URL (optional, nur bei Überwachungstypen *HTTP/S Host*): Anzufragende URL.Sie können statt den Standard-Ports 80 und 443 auch andere Ports verwenden, indem Sie die Port-Information an die URL anhängen, z. B. `http://beispiel.domaene:8080/index.html`. Wenn keine URL angegeben ist, wird das Wurzelverzeichnis angefragt.

Intervall: Geben Sie eine Zeitspanne in Sekunden an, in der die Hosts überprüft werden.

Zeitüberschreitung: Geben Sie einen maximalen Zeitraum in Sekunden an, in dem die überwachenden Hosts eine Antwort senden können. Wenn keiner der überwachenden Hosts einer Schnittstelle in diesem Zeitraum antwortet, wird die Schnittstelle als tot betrachtet.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

6.5 IPv6

Seit Version 8 unterstützt Sophos UTM IPv6, den Nachfolger von IPv4.

Die folgenden Funktionen von UTM unterstützen IPv6 ganz oder teilweise.

- Zugang zum WebAdmin und zum Benutzerportal
- SSH
- NTP
- SNMP
- SLAAC- (Stateless Address Autoconfiguration) und DHCPv6-Client-Unterstützung für alle dynamischen Schnittstellen
- DNS
- DHCP-Server
- BGP
- OSPF
- IPS
- Firewall

- NAT
- ICMP
- Server-Lastverteilung
- Webfilter
- Web Application Firewall
- SMTP
- IPsec (nur Site-to-Site)
- Syslog-Server

6.5.1 Allgemein

Auf der Registerkarte *IPv6 > Allgemein* können Sie die IPv6-Unterstützung für Sophos UTM aktivieren. Außerdem werden hier IPv6-Statusinformationen, z. B. Informationen über Präfix-Bekanntmachungen, angezeigt, wenn IPv6 aktiviert ist.

Die IPv6-Unterstützung ist standardmäßig ausgeschaltet. Um IPv6 zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie IPv6 auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün. Wenn IPv6 bisher noch nicht aktiviert oder konfiguriert wurde, ist im Abschnitt *Konnektivität* der Ausdruck *Keine* angegeben.

Sobald IPv6 aktiviert ist, werden Sie im WebAdmin viele Netzwerkdefinitionen und Definitionen von anderen Objekten vorfinden, die sich explizit auf IPv6 beziehen. Im Allgemeinen können Sie diese genauso verwenden, wie Sie es von den IPv4-Objekten gewöhnt sind.

Hinweis – Wenn IPv6 aktiviert ist, tragen die Symbole von Netzwerkobjekten eine zusätzliche Markierung, die Ihnen anzeigt, ob es sich bei dem jeweiligen Objekt um ein IPv6- oder ein IPv4-Objekt handelt oder um beides.

6.5.2 Präfix-Bekanntmachungen

Auf der Registerkarte *IPv6 > Präfix-Bekanntmachungen* können Sie Ihre Sophos UTM so konfigurieren, dass sie Clients ein IPv6-Adresspräfix zuweist, welches diesen dann ermöglicht, sich selbst eine IPv6-Adresse auszuwählen. Die Präfix-Bekanntmachung (prefix advertisement)

oder Router-Bekanntmachung (router advertisement) ist eine IPv6-Funktion, bei der sich Router (in diesem Fall die UTM) in gewisser Weise wie ein DHCP-Server unter IPv4 verhalten. Die Router weisen den Clients IPs jedoch nicht direkt zu.Stattdessen weisen sich die Clients in einem IPv6-Netzwerk eine sogenannte link-lokale Adresse für die erste Kommunikation mit dem Router zu. Der Router teilt dem Client dann das Präfix für dessen Netzwerksegment mit. Daraufhin generiert sich der Client eine IP-Adresse, die aus dem Präfix und seiner MAC-Adresse besteht.

Um ein neues Präfix anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Präfix-Bekanntmachungen* auf *Neues Präfix*.**
   Das Dialogfeld *Neues Präfix anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Schnittstelle: Wählen Sie eine Schnittstelle aus, die mit einer IPv6-Adresse und einer 64-Bit-Netzmaske konfiguriert ist.

   DNS-Server 1/2 (optional): Die IPv6-Adressen der DNS-Server.

   Domäne (optional): Tragen Sie den Domänennamen ein, der an die Clients übermittelt werden soll (z. B. `intranet.beispiel.de`).

   Gültige Lebensdauer: Der Zeitraum, für den das Präfix gültig sein soll. Der Standardwert ist 30 Tage.

   Bevorzugte Lebensdauer: Der Zeitraum, nach dem ein anderes Präfix, dessen bevorzugte Lebensdauer noch nicht vorüber ist, vom Client gewählt werden soll. Der Standardwert ist 7 Tage.

   Andere Konfig (optional): Diese Option ist standardmäßig ausgewählt. Sie stellt sicher, dass ein angegebener DNS-Server und ein Domänenname zusammen mit dem angegebenen Präfix über DHCPv6 bekannt gegeben werden. Dies ist nützlich, da es zurzeit zu wenig Clients gibt, die DNS-Informationen von den Präfix-Bekanntmachungen (RFC 5006/ RFC 6106) abrufen können. Beachten Sie, dass diese DHCPv6-Konfiguration versteckt verläuft und daher über das DHCP-Konfigurationsmenü weder sichtbar noch editierbar ist.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Präfix-Konfiguration wird in der Liste *Präfix-Bekanntmachungen* angezeigt.

6.5.3 Umnummerierung

Auf der Registerkarte *IPv6 > Umnummerierung* können Sie für den Fall einer Änderung des Präfixes die automatische Umnummerierung der durch die UTM verwalteten IPv6-Adressen erlauben. Außerdem können Sie IPv6-Adressen manuell umnummerieren.

Die folgenden IPv6-Adressen werden geändert:

- Host-, Netzwerk- und Bereichsdefinitionen
- Hauptadressen und zusätzliche Adressen von Schnittstellen
- DHCPv6-Server-Bereiche und -Zuordnungen
- DNS-Zuordnungen

IPv6-Präfixe, die durch den Tunnel-Broker zugewiesen wurden, werden nicht umnummeriert.

Automatische IPv6-Umnummerierung

Standardmäßig werden die durch Ihre UTM verwalteten IPv6-Adressen automatisch umnummeriert, wenn sich das IPv6-Präfix ändert. Präfixänderungen werden durch Ihren ISP über DHCPv6-Präfixdelegation ausgelöst. Um die Umnummerierung zu deaktivieren, deaktivieren Sie das Auswahlkästchen und klicken Sie auf *Übernehmen*.

Manuelle IPv6-Umnummerierung

Sie können bestimmte IPv6-Adressen, die durch die UTM verwaltet werden, manuell umnummerieren. Dies kann hilfreich sein, wenn Sie zu einem neuen ISP wechseln, der ein neues IPv6-Präfix statisch statt automatisch über DHCPv6 zuweist.

1. **Legen Sie das aktuelle Präfix der IPv6-Adressen fest, die umnummeriert werden sollen.**
   Geben Sie das Präfix in das Feld *Altes Präfix* ein.

2. **Legen Sie das neue Präfix fest.**
   Geben Sie das Präfix in das Feld *Neues Präfix* ein.

3. **Klicken Sie auf *Übernehmen*.**

   Alle IPv6-Adressen mit dem festgelegten aktuellen Präfix werden mit Hilfe des neuen Präfixes umnummeriert.

6.5.4 6to4

Auf der Registerkarte *IPv6 > 6to4* können Sie Sophos UTM so konfigurieren, dass IPv6-Adressen automatisch über ein vorhandenes IPv4-Netzwerk getunnelt werden. Bei 6to4 hat jede IPv4-Adresse ein `/48`-Präfix aus dem IPv6-Netzwerk, auf das sie abgebildet wird.Die daraus resultierende IPv6-Adresse besteht aus dem Präfix `2002` und der IPv4-Adresse in hexadezimaler Schreibweise.

> **Hinweis –** Sie können entweder *6to4* oder *Tunnel-Broker* aktiviert haben.

Um das Tunneln von IP-Adressen für eine bestimmte Schnittstelle zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie *6to4* auf der Registerkarte 6to4.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und die Abschnitte *6to4* sowie *Erweitert* können nun bearbeitet werden.

2. **Wählen Sie eine Schnittstelle aus.**
   Wählen Sie eine Schnittstelle aus der Auswahlliste *Schnittstelle*, die eine öffentliche IPv6-Adresse besitzt.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert. Der Schnittstellenstatus wird auf der Registerkarte *Allgemein*angezeigt.

Erweitert

Sie können die *Server-Adresse* ändern, um einen anderen 6to4-Relay-Server zu verwenden.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

6.5.5 Tunnel-Broker

Auf der Registerkarte *IPv6 > Tunnel-Broker* können Sie die Verwendung eines Tunnel-Broker aktivieren. Die Tunnelvermittlung (tunnel brokerage) ist ein Dienst, der von einigen ISPs angeboten wird, und es ermöglicht, über IPv6-Adressen auf das Internet zuzugreifen.

> **Hinweis –** Sie können entweder *6to4* oder *Tunnel-Broker* aktiviert haben.

Sophos UTMunterstützt die folgenden Tunnel-Broker (Vermittlungsdienste):

- Teredo (nur Anonymous)
- Freenet6 (nach GoGo6) (Anonymous oder mit Benutzerkonto)
- SixXS (Benutzerkonto erforderlich)

Um einen Tunnel-Broker zu verwenden, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die Tunnelvermittlung auf der Registerkarte *Tunnel-Broker*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und die Abschnitte *Tunnel-Broker* sowie *Erweitert* können nun bearbeitet werden. Der Tunnel-Broker ist sofort aktiv und verwendet Teredo mit anonymer Authentifizierung. Der Verbindungsstatus wird auf der Registerkarte *Allgemein* angezeigt.

Tunnel-Broker

Sie können die Standardeinstellungen für den Tunnel-Broker ändern.

Authentifizierung: Wählen Sie eine Authentifizierungsmethode aus der Auswahlliste.

- **Anonymous:** Bei dieser Methode benötigen Sie kein Benutzerkonto bei dem entsprechenden Broker. Die zugewiesene IP-Adresse ist jedoch nur temporär.
- **Benutzer:** Sie müssen sich bei dem entsprechenden Broker anmelden, um ein Benutzerkonto zu bekommen.

Broker: Wählen Sie einen anderen Broker aus der Auswahlliste aus.

Benutzername (nur bei *User* verfügbar): Geben Sie Ihren Benutzernamen für den entsprechenden Broker an.

Kennwort (nur bei *User* verfügbar): Geben Sie Ihr Kennwort für den Benutzernamen an.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Erweitert

Hier können Sie eine andere Serveradresse für den gewählten Tunnel-Broker angeben.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

6.6 Statisches Routing

Jeder an ein Netzwerk angeschlossener Computer verwendet eine Routing-Tabelle, mit deren Hilfe er feststellt, welchen Weg ein ausgehendes Datenpaket nehmen muss, um sein Ziel zu erreichen. Die Routing-Tabelle enthält z. B. Informationen darüber, ob sich eine Zieladresse im lokalen Netzwerk befindet oder ob das Datenpaket über einen Router weitergeleitet werden muss. Falls ein Router beteiligt ist, enthält die Tabelle die Information, welcher Router für welches Netzwerk benutzt werden muss.

Zwei Routenarten können zur Routing-Tabelle von Sophos UTM hinzugefügt werden: statische Routen und Richtlinienrouten. Bei statischen Routen werden die Routingziele lediglich von der Zieladresse der Datenpakete bestimmt. Bei Richtlinienrouten ist es möglich, das Routing anhand der Quellschnittstelle, der Absenderadresse, des Dienstes oder der Zieladresse zu bestimmen.

Hinweis – Sie brauchen für Netzwerke, die direkt an die Schnittstellen der UTM angeschlossen sind, sowie für Standardrouten keine Routing-Einträge anzulegen. Diese Routing-Einträge werden vom System automatisch erstellt.

6.6.1 Statische Routen

Für die direkt angeschlossenen Netzwerke trägt das System die entsprechenden Routing-Einträge selbst ein. Weitere Einträge müssen manuell vorgenommen werden, z. B. wenn im lokalen Netzwerk ein weiterer Router existiert, über den ein bestimmtes Netzwerk erreicht werden soll. Routen für Netzwerke, die nicht direkt angeschlossen sind, aber über einen Befehl oder eine Konfigurationsdatei in die Routing-Tabelle eingetragen werden, bezeichnet man als statische Routen.

Um eine statische Route hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Statische Routen* auf *Neue statische Route.***
   Das Dialogfeld *Neue statische Route erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

   Routentyp: Die folgenden Routentypen sind verfügbar:

- **Schnittstellen-Route:** Datenpakete werden an eine bestimmte Schnittstelle geschickt. Dieser Typ kann in zwei Fällen nützlich sein: Für Routing-Einträge zu dynamischen Schnittstellen (z. B. PPP), da in diesem Fall die IP-Adresse des Gateways nicht bekannt ist, oder für eine Standard-Route mit einem Gateway außerhalb der direkt angeschlossenen Netzwerke.
- **Gateway-Route:** Die Datenpakete werden an einen bestimmten Host (Gateway) geschickt.
- **Blackhole-Route:** Die Datenpakete werden ohne Rückmeldung an den Absender verworfen. In Verbindung mit OSPF oder anderen dynamischen adaptiven Routing-Protokollen können dadurch unter anderem „Routing Loops“ (Schleifen) oder „Route Flapping“ (schnelles Wechseln von Routen) verhindert werden.

Netzwerk: Wählen Sie die Zielnetzwerke der Datenpakete, die die UTM abfangen muss.

Schnittstelle: Wählen Sie die Schnittstelle, durch die die Datenpakete die UTM verlassen (nur verfügbar, wenn Sie *Schnittstellenroute* als Routentyp gewählt haben).

Gateway: Wählen Sie das Gateway/den Router aus, an das oder den UTM die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Gateway-Route* als Routentyp gewählt haben).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgende erweiterte Einstellung vornehmen:**
   Metrik: Geben Sie einen Metrikwert ein. Dieser kann eine Ganzzahl zwischen 0 und 4294967295 sein. Der Standardwert beträgt 5. Dieser Metrikwert wird verwendet, um Routen, die zum selben Ziel führen, zu unterscheiden und zu priorisieren. Ein niedriger Metrikwert wird einem hohen Metrikwert vorgezogen. IPsec-Routen besitzen automatisch den Metrikwert 0.
4. **Klicken Sie auf *Speichern*.**
   Die neue Route wird in der Liste *Statische Routen* angezeigt.
5. **Aktivieren Sie die Route.**
   Klicken Sie auf den Schieberegler, um die Route zu aktivieren.

Um eine Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.6.2 Richtlinienrouten

Normalerweise entscheidet ein Router darüber, wohin ein bestimmtes Paket geschickt werden muss, indem er die Zieladresse im Paket selbst ausliest und den entsprechenden Eintrag in einer Routing-Tabelle nachschaut. Manchmal jedoch ist es notwendig ein Paket basierend auf anderen Kriterien weiterzuleiten. Das richtlinienbasierte Routing ermöglicht die Weiterleitung bzw. das Routen von Datenpaketen nach eigenen Sicherheitsrichtlinien.

Um eine Richtlinienroute hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Richtlinienrouten* auf *Neue Richtlinienroute*.**
   Das Dialogfeld *Neue Richtlinienroute erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Position: Die Positionsnummer legt die Priorität der Richtlinienroute fest. Niedrigere Nummern haben eine höhere Priorität. Routen werden in aufsteigender Reihenfolge abgeglichen. Sobald eine Route zutrifft, werden Routen mit einer höheren Nummer nicht mehr abgeglichen.

   Routentyp: Die folgenden Routentypen sind verfügbar:

   - **Schnittstellen-Route:** Datenpakete werden an eine bestimmte Schnittstelle geschickt. Dieser Typ kann in zwei Fällen nützlich sein: Für Routing-Einträge zu dynamischen Schnittstellen (z. B. PPP), da in diesem Fall die IP-Adresse des Gateways nicht bekannt ist, oder für eine Standard-Route mit einem Gateway außerhalb der direkt angeschlossenen Netzwerke.

   - **Gateway-Route:** Die Datenpakete werden an einen bestimmten Host (Gateway) geschickt.

   Quellschnittstelle: Die Schnittstelle, auf der das zu routende Datenpaket ankommt.Mit der Einstellung *Any* werden alle Schnittstellen geprüft.

   Quellnetzwerk: Das Quellnetzwerk des zu routenden Datenpakets. Mit der Einstellung *Any* werden alle Netzwerke geprüft.

   Dienst: Datenpakete dieses Diensts werden auf passende Routing-Regeln geprüft. Die Auswahlliste enthält sowohl die vordefinierten als auch Ihre selbst definierten Dienste. Mit Hilfe dieser Dienste lässt sich präzise definieren, welche Art von Datenverkehr verarbeitet werden soll. Die Einstellung *Any* entspricht in diesem Fall allen Kombinationen aus Protokollen und Quell- bzw. Zielports.

Zielnetzwerk: Das Zielnetzwerk des zu routenden Datenpakets. Mit der Einstellung *Any* werden alle Netzwerke geprüft.

Zielschnittstelle: Die Schnittstelle, an die die Datenpakete gesendet werden (nur verfügbar, wenn Sie als Routentyp *Schnittstellen-Route* gewählt haben).

Gateway: Wählen Sie das Gateway/den Router aus, an das oder den das Gateway die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Gateway-Route* als Routentyp gewählt haben).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Route wird in der Liste *Richtlinienrouten* angezeigt.

4. **Aktivieren Sie die Route.**
   Klicken Sie auf den Schieberegler, um die Route zu aktivieren.

Um eine Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.7 Dynam. Routing (OSPF)

Das Protokoll *Open Shortest Path First* (OSPF) ist ein dynamisches Link-State-Routing-Protokoll, das hauptsächlich innerhalb von großen autonomen Systemnetzwerken genutzt wird. Sophos UTM unterstützt OSPF Version 2. Im Gegensatz zu anderen Protokollen nutzt OSPF die Kosten für die Pfade als Routing-Metrik. Die Kosten für die Übermittlung von Datenpaketen über eine Schnittstelle mit eingeschaltetem OSPF werden aus der verfügbaren Bandbreite berechnet. Dabei sind die Kosten umgekehrt proportional zu der verfügbaren Bandbreite der Schnittstelle – eine größere Bandbreite hat somit geringere Kosten zur Folge. Die Kosten und die entstehende Zeitverzögerung sind z. B. bei einer seriellen Schnittstelle mit 56 Kbit/s höher als bei einer Ethernet-Schnittstelle mit 10 Mbit/s.

Die OSPF-Spezifikation enthält keine Angaben darüber, wie die Kosten für ein angeschlossenes Netzwerk berechnet werden – dies wird dem Anbieter überlassen. Daher können Sie eine eigene Berechnungsformel für die Kosten definieren. Wenn das OSPF-Netzwerk jedoch an ein anderes Netzwerk angrenzt, bei dem bereits eine Formel definiert wurde, muss diese hier ebenfalls als Basis für die Kostenberechnung verwendet werden.

Die Kosten werden standardmäßig bandbreitenbasiert berechnet. Cisco beispielsweise berechnet die Kosten folgendermaßen: 10^8 dividiert durch die Schnittstellen-Bandbreite in Bit pro Sekunde. Laut dieser Formel betragen die Kosten, um eine 10-Mbit/s-Ethernet-Schnittstelle zu benutzen, 10^8/10.000.000 = 10 und 10^8/1.544.000 = 64, um eine 1,544-Mbit/s-Schnittstelle (T1) zu benutzen (ungerade Ergebnisse werden auf eine Ganzzahl abgerundet).

6.7.1 Allgemein

Auf der Registerkarte *Schnittstellen & Routing > Dynamisches Routing (OSPF) > Allgemein* werden die Grundeinstellungen für OSPF vorgenommen. Bevor Sie die OSPF-Funktion aktivieren können, müssen Sie mindestens einen OSPF-Bereich konfigurieren (auf der Registerkarte *Bereich*).

Achtung – Die Einstellungen für die OSPF-Funktion von Sophos UTM sollten nur von einem technisch erfahrenen Administrator durchgeführt werden, der mit dem Protokoll OSPF vertraut ist. Die Konfigurationsbeschreibungen in diesem Kapitel umfassen nicht genügend Aspekte von OSPF, um ein umfassendes Verständnis des OSPF-Protokolls zu erreichen. Verwenden Sie diese Funktion deshalb mit Vorsicht, da eine fehlerhafte Konfiguration das Netzwerk betriebsunfähig machen kann.

Um OSPF zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Konfigurieren Sie auf der Registerkarte *Bereich* mindestens einen OSPF-Bereich.**

2. **Aktivieren Sie OSPF auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Router* kann nun bearbeitet werden.

3. **Geben Sie die Router-ID ein.**
   Geben Sie eine eindeutige ID ein, über die sich Sophos UTM gegenüber den anderen OSPF-Routern identifiziert.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um OSPF zu deaktivieren, klicken Sie auf den Schieberegler.

6.7.2 Bereich

Ein OSPF-Netzwerk ist in mehrere Bereiche unterteilt. Dies sind logische Gruppierungen von Routern, deren Informationen für das restliche Netzwerk zusammengefasst werden können. Die einzelnen Bereiche werden durch eine 32-Bit-ID in der Punkt-Dezimalschreibweise festgelegt – ähnlich der Schreibweise bei IP-Adressen.

Es gibt insgesamt sechs OSPF-Bereichstypen:

- **Backbone:** Der Bereich mit der ID 0 (oder `0.0.0.0`) ist für das Backbone-Netzwerk des OSPF-Netzwerks reserviert, welches das Kernnetz eines OSPF-Netzwerks bildet – alle anderen Bereiche sind damit verbunden.
- **Normal:** Ein normaler oder regulärer Bereich erhält eine eindeutige ID im Bereich 1 (oder `0.0.0.1`) bis 4.294.967.295 (oder `255.255.255.255`). In normalen Bereichen werden externe Routen bidirektional über den *Area Border Router* (ABR, Grenzrouter) geflutet. Beachten Sie, dass externe Routen als Routen definiert werden, die im OSPF von einem anderen Routing-Protokoll verteilt werden.
- **Stub:** Ein Stub-Bereich hat üblicherweise keine direkte Verbindung zu einem externen Netzwerk. Das Zuführen externer Routen in einen Stub-Bereich ist nicht erforderlich, da sämtlicher Datenverkehr in externe Netzwerke durch einen *Area Border Router* (ABR) geleitet werden muss. Daher ersetzt der Stub-Bereich eine vorgegebene Route durch externe Routen, um Daten an externe Netzwerke zu senden.
- **Stub No-Summary:** Der Bereich *Stub No-Summary* (auch *Totally Stubby Area*) ist mit einem Stub-Bereich vergleichbar, allerdings werden keine sogenannten Summary Routes erlaubt. Das bedeutet, dass die Flutung von Summary-Link-State-Advertisements (LSAs) des Typs 3 in dem Bereich damit eingeschränkt wird.
- **NSSA:** Dieser Bereich (Not-So-Stubby-Area/NSSA) ist eine Art von Stub-Bereich, in dem allerdings auch externe Verbindungen unterstützt werden. Beachten Sie dabei, dass keine virtuellen Links unterstützt werden.
- **NSSA No-Summary:** Dieser Bereich (*NSSA No-Summary*) ist mit NSSA vergleichbar, allerdings werden keine sogenannten Summary Routes erlaubt. Das bedeutet, dass die Flutung von Summary-Link-State-Advertisements (LSAs) des Typs 3 in dem Bereich damit eingeschränkt wird.

Um einen OSPF-Bereich anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Bereich* auf *Neuer OSPF-Bereich*.**
   Das Dialogfeld *Neuen OSPF-Bereich erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den Bereich ein.

   Bereich-ID: Tragen Sie die ID für den Bereich in der Punkt-Dezimalschreibweise ein (z. B. `0.0.0.1` für einen normalen Bereich oder `0.0.0.0` für den Backbone-Bereich).

   Bereichstyp: Wählen Sie einen Bereichstyp (siehe obige Beschreibung) aus, um die Charakteristika des Netzwerks festzulegen, dem dieser Bereich zugewiesen wird.

   Auth.-Methode: Wählen Sie für alle Pakete, die über die Schnittstelle den OSPF-Bereich erreichen, die Authentifizierungsmethode aus. Die folgenden Authentifizierungsmethoden sind verfügbar:

   - **MD5:** Diese Option aktiviert die MD5-Authentifizierung. MD5 (Message-Digest Algorithm 5) ist eine weit verbreitete kryptografische Hash-Funktion, die einen 128-Bit-Hashwert benutzt.
   - **Klartext:** Diese Option aktiviert die Klartext-Authentifizierung. Das Kennwort wird als Klartext durch das Netzwerk geschickt.
   - **Aus:** Diese Option deaktiviert die Authentifizierung.

   Verbinden über Schnittstelle: Wählen Sie eine OSPF-Schnittstelle aus.Beachten Sie, dass OSPF-Schnittstellen, die Sie hier spezifizieren, vorher auf der Registerkarte *Schnittstellen* erstellt worden sein müssen.

   Virtuelle Links verbinden: Alle Bereiche in einem *autonomen OSPF-System* (AS) müssen physisch mit dem Backbone-Bereich (Bereich 0) verbunden sein. In manchen Fällen, wenn eine physikalische Verbindung nicht möglich ist, können Sie einen virtuellen Link verwenden, um den Backbone-Bereich mit einem Nicht-Backbone-Bereich zu verbinden. Geben Sie im Feld *Virtuelle Links verbinden* die Router-ID, die dem virtuellen Link-Nachbarn zugeordnet ist, in der Punkt-Dezimalschreibweise ein (z. B. `10.0.0.8`).

   Kosten: Die Kosten für das Senden und Empfangen von Datenpaketen in diesem Bereich. Gültige Werte für Kosten liegen im Bereich 1 bis 65535.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Bereichsdefinition wird auf der Registerkarte *Bereich* angezeigt.

Um einen OSPF-Bereich zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Im OSPF-Live-Protokoll werden die Aktivitäten auf der OSPF-Schnittstelle protokolliert. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

6.7.3 Schnittstellen

Auf der Registerkarte *Schnittstellen & Routing > Dynamisches Routing (OSPF) > Schnittstellen* können Sie Schnittstellendefinitionen erstellen, die innerhalb eines OSPF-Bereichs genutzt werden sollen. Jede Definition enthält verschiedene Parameter, die spezifisch für OSPF-Schnittstellen sind.

Um eine OSPF-Schnittstellendefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue OSPF-Schnittstelle*.**
   Das Dialogfeld *Neue OSPF-Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Schnittstelle ein.

   Schnittstelle: Wählen Sie die Schnittstelle aus, die der OSPF-Schnittstellendefinition zugeordnet werden soll.

   Auth.-Methode: Wählen Sie die Authentifizierungsmethode aus, die für alle OSPF-Pakete verwendet werden soll, die über die Schnittstelle gesendet und empfangen werden. Die folgenden Authentifizierungsmethoden sind verfügbar:

   - **MD5:** Diese Option aktiviert die MD5-Authentifizierung. MD5 (Message-Digest Algorithm 5) ist eine weit verbreitete kryptografische Hash-Funktion, die einen 128-Bit-Hashwert benutzt.

   - **Klartext:** Diese Option aktiviert die Klartext-Authentifizierung. Das Kennwort wird als Klartext durch das Netzwerk geschickt.

   - **Aus:** Diese Option deaktiviert die Authentifizierung.

   Prüfsumme: Wählen Sie die Prüfsumme (MD, Message Digest), um die MD5-Authentifizierung für diese OSPF-Schnittstelle festzulegen. Beachten Sie, dass Sie eine Prüfsumme zunächst auf der Registerkarte *Prüfsummen* anlegen müssen, bevor Sie sie hier auswählen können.

Kosten: Die Kosten für die Übermittlung von Datenpaketen über diese Schnittstelle. Gültige Werte für Kosten liegen im Bereich 1 bis 65535.

Erweiterte Optionen (optional): Durch die Auswahl der Option *Erweiterte Optionen* werden weitere Konfigurationsoptionen angezeigt:

- **Grußpaketintervall:** Legen Sie das Zeitintervall fest (in Sekunden), das Sophos UTM wartet, bevor es *Grußpakete* über diese Schnittstelle sendet. Als Standardwert sind zehn Sekunden voreingestellt.
- **Wiederübertragungsintervall:** Legen Sie das Zeitintervall (in Sekunden) fest, nach dem ein LSA (Link State Advertisement) für die Schnittstelle nochmals übertragen wird, wenn keine Bestätigung eingegangen ist. Es ist ein Zeitintervall von fünf Sekunden voreingestellt.
- **Totes Intervall:** Legen Sie das Zeitintervall fest (in Sekunden), das Sophos UTM auf *Grußpakete* wartet, die über die Schnittstelle eintreffen. Als Standardwert sind 40 Sekunden voreingestellt. Per Konvention muss der Wert des *toten Intervalls* grundsätzlich vier mal größer sein als der Wert des *Grußpaketintervalls*.
- **Priorität:** Legen Sie die Router-Priorität fest, bei der es sich um eine 8-Bit-Nummer zwischen 1 und 255 handelt, die hauptsächlich dafür genutzt wird, um in einem Netzwerk den designierten Router (DR, Designated Router) zu bestimmen. Als Standardwert ist 1 voreingestellt.
- **Übertragungsverzögerung:** Legen Sie das geschätzte Zeitintervall (in Sekunden) fest, das benötigt wird, um ein Link-State-Update-Paket (Linkstatus-Aktualisierung) über die Schnittstelle zu senden. Gültige Werte liegen im Bereich 1 bis 65535; als Standardwert ist 1 voreingestellt.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die OSPF-Schnittstellendefinition wird auf der Registerkarte *Schnittstellen* angezeigt.

Um eine OSPF-Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Im OSPF-Live-Protokoll werden die Aktivitäten auf der OSPF-Schnittstelle protokolliert. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

6.7.4 Prüfsummen

Auf der Registerkarte *Schnittstellen & Routing > Dynamisches Routing (OSPF) > Prüfsummen* werden sogenannte Prüfsummenschlüssel generiert. Prüfsummenschlüssel sind erforderlich, um die MD5-Authentifizierung mit OSPF zu aktivieren. Die MD5-Authentifizierung generiert eine 128-Bit-Prüfsumme aus Datenpaket und Kennwort. Die Prüfsumme wird mit dem Datenpaket und einer Schlüssel-ID verschickt, welche dem Kennwort zugeordnet ist.

Hinweis – Auf allen empfangenden Routern muss derselbe Prüfsummenschlüssel konfiguriert sein.

Um einen Prüfsummenschlüssel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Prüfsummen* auf *Neuer Prüfsummenschlüssel*.**
   Das Dialogfeld *Neuen Prüfsummenschlüssel erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   ID: Tragen Sie die Schlüssel-Identifikationsnummer für diesen Prüfsummenschlüssel ein. Gültige Werte liegen im Bereich zwischen 1 und 255.

   MD5-Schlüssel: Tragen Sie das Kennwort ein. Es kann bis zu 16 alphanumerische Zeichen enthalten.
3. **Klicken Sie auf *Speichern*.**
   Der neue Schlüssel wird in der Liste *Prüfsummen* angezeigt.

Um einen Prüfsummenschlüssel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.7.5 Fehlersuche

Auf der Registerkarte *Schnittstellen & Routing > Dynamisches Routing (OSPF) > Fehlersuche* werden detaillierte Informationen zu relevanten OSPF-Parametern in einem separaten Browser-Fenster dargestellt. Die folgenden Informationen sind verfügbar:

- **IP des OSPF-Nachbarn anzeigen:** Es werden schnittstellenbezogene Informationen zu den OSPF-Neighbors angezeigt.

- **IP der OSPF-Routen anzeigen:** Es wird der aktuelle Stand der Routing-Tabelle angezeigt.
- **IP der OSPF-Schnittstelle anzeigen:** Es werden OSPF-bezogene Schnittstelleninformationen angezeigt.
- **IP der OSPF-Datenbank anzeigen:** Es werden zu einem bestimmten Router OSPF-datenbankbezogene Informationen anzeigt.
- **IP der OSPF-Grenzrouter anzeigen:** Es werden die internen Einträge aus der OSPF-Routing-Tabelle zum *Area Border Router* (ABR) und zum *Autonomous System Boundary Router* (ASBR) angezeigt.

6.7.6 Erweitert

Auf der Registerkarte *Schnittstellen & Routing > Dynamisches Routing (OSPF) > Erweitert* befinden sich die erweiterten Einstellungen für OSPF. Die Funktionen beziehen sich dabei auf die Einspeisung (Neuverteilung) von Routing-Informationen aus einer Nicht-OSPF-Domäne in die OSPF-Domäne.

Hinweis – Richtlinienrouten können nicht neu verteilt werden.

Verbundene neu verteilen: Um die Routen von direkt verbundenen Netzwerken neu zu verteilen, wählen Sie diese Option aus. Der Metrikwert (Kostenfaktor) 10 ist voreingestellt.

Statische neu verteilen: Um statische Routen neu zu verteilen, wählen Sie diese Option aus.

Hinweis – Für IPsec-Tunnel muss *Striktes Routing* deaktiviert sein, um eine Neuverteilung zu ermöglichen (siehe Kapitel Verbindungen).

IPsec neu verteilen: Um IPsec-Routen neu zu verteilen, wählen Sie diese Option aus. Die Option *bind to interface* sollte deaktiviert sein.

SSL VPN neu verteilen Um SSL-VPN-Routen neu zu verteilen, wählen Sie diese Option aus. Der Metrikwert (Kostenfaktor) 10 ist voreingestellt.

BGP neu verteilen Um BGP-Routen neu zu verteilen, wählen Sie diese Option aus. Der Metrikwert (Kostenfaktor) 10 ist voreingestellt.

Standardroute bekannt geben: Um eine vorgegebene Route zur OSPF-Domäne neu zu verteilen, wählen Sie diese Option aus.

Hinweis – Eine vorgegebene Route wird in der OSPF-Domäne angezeigt, ungeachtet dessen, ob sie eine Route zu `0.0.0.0/0` enthält.

Schnittstellen-Linkerkennung: Wählen Sie diese Option aus, wenn Routen auf Schnittstellen nur dann bekannt gegeben werden sollen, wenn ein Link mit der Schnittstelle erkannt wird.

6.8 Border Gateway Protocol

Das Border Gateway Protocol (BGP) ist ein Routing-Protokoll, das hauptsächlich von Internetanbietern (ISPs) verwendet wird, um die Kommunikation zwischen mehreren autonomen Systemen (Autonomous System, AS) zu ermöglichen, das heißt zwischen mehreren ISPs. Dadurch bildet BGP das Rückgrat des Internets. Ein autonomes System besteht aus mehreren miteinander verbundenen IP-Netzwerken, die von einem oder mehreren ISPs kontrolliert werden und über ein internes Routing-Protokoll (z. B. IGP) miteinander verbunden sind. BGP wird als Pfad-Vektor-Protokoll bezeichnet und trifft seine Routing-Entscheidungen, im Gegensatz zu IGP, anhand von Pfad, Netzwerkrichtlinien und/oder Regelwerken. Aus diesem Grund könnte man es eher als Erreichbarkeitsprotokoll bezeichnen denn als Routing-Protokoll.

Jeder ISP (oder andere Netzwerkanbieter) muss im Besitz einer offiziell registrierten AS-Nummer (Autonomous System Number, ASN) sein, um sich selbst im Netzwerk ausweisen zu können. Obwohl ein ISP intern mehrere autonome Systeme unterstützen mag, ist für das Internet nur das Routing-Protokoll relevant. AS-Nummern aus dem Bereich 64512–65534 sind privat und können nur intern verwendet werden.

BGP verwendet TCP als Transportprotokoll, auf Port 179.

Wenn BGP zwischen Routern eines einzigen AS verwendet wird, spricht man von internem BGP (interior BGP, iBGP); wenn es hingegen zwischen Routern von verschiedenen AS verwendet wird, spricht man von externem BGP (exterior BGP, eBGP).

Eine Stärke von eBGP ist seine Fähigkeit, Routing-Schleifen zu verhindern, das heißt, dass ein IP-Paket ein AS niemals zweimal passiert. Dies wird folgendermaßen erreicht: Ein eBGP-Router pflegt eine komplette Liste aller AS, die ein IP-Paket passieren muss, um ein bestimmtes Netzwerksegment zu erreichen. Wenn der Router sendet, teilt er diese Information mit seinen eBGP-Nachbarroutern (neighbors), welche daraufhin ihre Routingliste aktualisieren, falls nötig. Wenn ein eBGP-Router feststellt, dass er bereits auf einer solchen UPDATE-Liste eingetragen ist, fügt er sich nicht noch einmal hinzu.

6.8.1 Allgemein

Auf der Seite *Border Gateway Protocol > Allgemein* können Sie BGP für die UTM aktivieren und deaktivieren.

1. **Um BGP aktivieren zu können, legen Sie auf der Seite *Neighbor* mindestens einen Neighbor an.**
2. **Aktivieren Sie auf der Seite *Allgemein* BGP.**
   Klicken Sie auf den Schieberegler. Der Schieberegler wird gelb und der Abschnitt *BGP-System* kann nun bearbeitet werden.
3. **Nehmen Sie die folgenden Einstellungen vor:**
   AS-Nummer: Geben Sie die AS-Nummer (Autonomous System Number, ASN) Ihres Systems ein.

   Router-ID: Geben Sie eine IPv4-Adresse als Router-ID ein, die den Neighbors während der Sitzungsinitialisierung übermittelt wird.

   Netzwerke: Fügen Sie die Netzwerke hinzu, die den Neighbors vom System bekannt gegeben werden sollen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.
4. **Klicken Sie auf *Übernehmen*.**

   Der Schieberegler wird grün und BGP wird aktiviert. Schon bald werden im Bereich *BGP-Zusammenfassung* Statusinformationen angezeigt.

6.8.2 Systeme

Auf der Seite *Border Gateway Protocol > Systeme* können Sie eine Umgebung mit mehreren autonomen Systemen einrichten.

Hinweis – Diese Seite ist nur zugänglich, wenn Sie die Verwendung von mehreren AS auf der Seite *Erweitert* aktivieren.

Um ein neues BGP-System anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Systeme* auf *Neues BGP-System*.**
   Das Dialogfeld *Neues BGP-System anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für das System ein.

   ASN: Geben Sie die AS-Nummer (Autonomous System Number, ASN) Ihres Systems ein.

   Router-ID: Geben Sie eine IPv4-Adresse als Router-ID ein, die den Neighbors während der Sitzungsinitialisierung übermittelt wird.

   Neighbor: Markieren Sie die Auswahlkästchen derjenigen Neighbors, die zum AS dieses Systems gehören. Beachten Sie, dass Sie die Neighbors zuvor auf der Seite *Neighbor* anlegen müssen.

   Netzwerke: Fügen Sie die Netzwerke hinzu, die vom System bekannt gegeben werden sollen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Routen installieren: Diese Option ist standardmäßig aktiviert und sollte nur deaktiviert werden, wenn Sie wollen, dass ein BGP-Router die Routen kennt, aber nicht aktiv am BGP-Routing-Prozess teilnimmt. Wenn es mehrere AS-Systeme gibt, auf denen diese Option aktiviert ist, müssen Filterlisten angelegt werden, um sicherzustellen, dass es keine doppelten Netzwerke gibt. Andernfalls ist das Routing-Verhalten für identische Netzwerke unbestimmt.

3. **Klicken Sie auf *Speichern*.**
   Das System wird in der Liste *Systeme* angezeigt.

6.8.3 Neighbor

Auf der Seite *Border Gateway Protocol > Neighbor* können Sie einen oder mehrere BGP-Neighbor-Router anlegen. Ein Nachbarrouter (neighbor oder peer router) stellt die Verbindung zwischen mehreren autonomen Systemen (AS) oder innerhalb eines einzigen AS her. Während der ersten Kommunikation tauschen zwei Neighbors ihre BGP-Routing-Tabellen miteinander aus. Danach senden sie sich gegenseitig Aktualisierungen bei Änderungen in der Routing-Tabelle zu. Pakete zur Aufrechterhaltung der Verbindung (keepalive packets) werden versendet, um sicherzustellen, dass die Verbindung nach wie vor besteht. Sollten Fehler auftreten, werden Benachrichtigungen (notifications) versendet.

Richtlinien-Routing in BGP unterscheidet zwischen Richtlinien für eingehenden und ausgehenden Verkehr. Dies ist der Grund dafür, dass Routemaps und Filterlisten getrennt auf eingehenden und ausgehenden Verkehr angewendet werden können.

Sie müssen mindestens einen Neighbor-Router anlegen, bevor Sie BGP auf der Seite *Allgemein* aktivieren können.

Um einen neuen BGP-Neighbor anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Neighbor* auf *Neuer BGP-Neighbor*.**
   Das Dialogfeld *Neuen BGP-Neighbor anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie den Namen des BGP-Neighbor-Routers ein.

   Host: Fügen Sie die Hostdefinition des Neighbors hinzu. Die festgelegte IP-Adresse muss von der UTM erreichbar sein. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Entfernte ASN: Geben Sie die AS-Nummer (Autonomous System Number, ASN) des Neighbors ein.

   Authentifizierung: Falls der Neighbor Authentifizierung erfordert, wählen Sie *TCP-MD5-Signatur* aus der Auswahlliste aus und geben Sie das Kennwort ein. Dieses muss mit dem Kennwort übereinstimmen, das auf dem Neighbor festgelegt wurde.

3. **Nehmen Sie die folgenden erweiterten Einstellungen vor, falls erforderlich.**
   Eingehende/Ausgehende Route: Falls Sie eine Routemap angelegt haben, können Sie diese hier auswählen. Mit *Eingehend* oder *Ausgehend* legen Sie fest, ob Sie die Routemap auf ein- oder ausgehende Meldungen anwenden möchten.

   Eingehender/Ausgehender Filter: Falls Sie eine Filterliste angelegt haben, können Sie diese hier auswählen. Mit *Eingehend* oder *Ausgehend* legen Sie fest, ob Sie den Filter auf ein- oder ausgehende Meldungen anwenden möchten.

   Next-Hop-Self: Wenn ein Router in einem iBGP-Netzwerk ein externes eBGP-Netzwerk bekannt gibt, wissen iBGP-Router, die über keine eigene direkte externe Verbindung verfügen, nicht, wie sie Pakete zu diesem Netzwerk routen sollen. Durch Auswählen dieser Option jedoch macht der eBGP-Router sich selbst als Gateway zum externen Netzwerk bekannt.

   Multihop: In einigen Fällen kann ein Cisco-Router eBGP gemeinsam mit einem Router eines Drittherstellers ausführen, der keine direkte Verbindung zwischen den beiden externen Peers erlaubt. Um die Verbindung zu ermöglichen, nutzen Sie den eBGP Multihop. Der eBGP-Multihop erlaubt eine Neighbor-Verbindung zwischen zwei externen Peers, die keine direkte Verbindung besitzen. Multihop ist nur für eBGP, nicht für iBGP, bestimmt.

Soft-Reconfiguration: Standardmäßig aktiviert. Diese Option ermöglicht das Speichern von Updates, die vom Neighbor gesendet wurden.

Default-Originate: Sendet die Standardroute 0.0.0.0 an den Neighbor. Der Neighbor verwendet diese Route nur, falls er ein Netzwerk erreichen muss, das nicht Teil seiner Routing-Tabelle ist.

Gewichtung: Cisco-spezifische Option. Legt ein generisches Gewicht für alle Routen fest, die durch diesen Neighbor gelernt wurden. Sie können einen Wert zwischen 0 und 65535 eingeben. Die Route mit dem höchsten Gewicht wird genommen, um ein bestimmtes Netzwerk zu erreichen. Das hier angegebene Gewicht überlagert ein Routemap-Gewicht.

4. **Klicken Sie auf *Speichern*.**
   Der Neighbor wird in der Liste *Neighbor* angezeigt.

6.8.4 Routemap

In BGP ist route-map ein Befehl, um Bedingungen für die Neuverteilung von Routen festzulegen und Richtlinien-Routing zu ermöglichen. Auf der Seite *Border Gateway Protocol > Routemap* können Sie Routemaps für bestimmte Netzwerke erstellen und Metriken, Gewichtungen bzw. Präferenzwerte einstellen.

Der Best-Path-Algorithmus, der festlegt, welche Route genommen wird, funktioniert folgendermaßen:

1. Gewicht wird überprüft.*
2. Lokale Präferenz wird überprüft.*
3. Lokale Route wird überprüft.
4. AS-Pfadlänge wird überprüft.
5. Ursprung wird überprüft.
6. Metrik wird überprüft.*

Dies ist nur eine Kurzbeschreibung. Da die Berechnung des Best Path sehr komplex ist, ziehen Sie für detaillierte Informationen bitte die einschlägige Dokumentation zu Rate, welche im Internet zur Verfügung steht.

Die Elemente, die mit einem Asterisk (*) markiert sind, können direkt konfiguriert werden.

Um eine BGP-Routemap anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Routemap* auf *Neue BGP-Routemap*.**
   Das Dialogfeld *Neue BGP-Routemap anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Routemap ein.

   Abgleich über: Wählen Sie aus, ob die Routemap die IP-Adresse eines bestimmten Routers oder ein ganzes AS vergleichen soll.

   - **IP-Adresse:** Im Feld *Netzwerke* können Sie Hosts oder Netzwerke hinzufügen oder auswählen, auf die der Filter angewendet werden soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   - **AS-Nummer:** Setzen Sie im Feld *AS-Regex* reguläre BGP-Ausdrücke ein, um AS-Nummern zu definieren, auf die der Filter angewendet werden soll. Beispiel: `_100_` stimmt mit jeder Route durch AS100 überein.

   Netzwerke: Fügen Sie Netzwerke und/oder Hosts hinzu, auf welche die Routemap angewendet werden soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Metrik: Standardmäßig lernt ein Router Routing-Metriken dynamisch. Sie können jedoch Ihren eigenen Metrikwert festlegen, der eine Ganzzahl zwischen 0 und 4294967295 sein kann. Ein niedriger Metrikwert wird einem hohen Metrikwert vorgezogen.

   Gewichtung: Die Gewichtung wird verwendet, um den besten Pfad auszuwählen. Sie wird für einen bestimmten Router festgelegt und nicht verbreitet. Wenn es mehrere Routen zu demselben Ziel gibt, werden Routen mit einer höheren Gewichtung bevorzugt. Die Gewichtung basiert auf dem zuerst zutreffenden AS-Pfad und kann eine Ganzzahl zwischen 0 und 4294967295 sein.

   > **Hinweis –** Falls einem Neighbor eine Gewichtung zugewiesen wurde, überlagert diese Gewichtung die Routemap-Gewichtung, wenn die Route mit dem angegebenen Netzwerk übereinstimmt.

   Präferenz: Sie können einen Präferenzwert für den AS-Pfad festlegen, welcher nur an alle Router im lokalen AS gesendet wird. Die Präferenz (oder lokale Präferenz) teilt den Routern in einem AS mit, welcher Pfad bevorzugt gewählt werden soll, um ein bestimm-

tes Netzwerk außerhalb des AS zu erreichen. Sie kann eine Ganzzahl zwischen 0 und 4294967295 sein und der Standardwert ist 100.

AS-Präfix: Das AS-Präfix wird eingesetzt, wenn aus irgendwelchen Gründen die Präferenz-Einstellungen nicht ausreichen, um eine bestimmte Route zu vermeiden, zum Beispiel eine Ersatzroute, die nur dann verwendet werden soll, wenn die Hauptroute nicht verfügbar ist. Damit können Sie das AS-Pfadattribut erweitern, indem Sie Ihre eigene AS-Nummer wiederholen, z. B. `65002 65002 65002`. Dies beeinflusst die Auswahl der BGP-Route, da der kürzeste AS-Pfad bevorzugt wird. Beachten Sie, dass Routemaps mit eingestelltem AS-Präfix im Feld *Ausgehende Route* eines Neighbors ausgewählt werden müssen, damit sie wie vorgesehen funktionieren.

3. **Klicken Sie auf *Speichern*.**
   Die Routemap wird in der Liste *Routemap* angezeigt.

Sie können die Routemap jetzt in einer Neighbor-Definition verwenden.

6.8.5 Filterliste

Auf der Seite *Border Gateway Protocol > Filterliste* können Sie Filterlisten anlegen, die dazu verwendet werden, den Verkehr zwischen Netzwerken anhand der IP-Adresse oder AS-Nummer zu regulieren.

Um eine Filterliste anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Filterliste* auf *Neue BGP-Filterliste*.**
   Das Dialogfeld *Neue BGP-Filterliste anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Filterliste ein.

   Filtern nach: Wählen Sie aus, ob der Filter die IP-Adresse eines bestimmten Routers oder ein ganzes AS vergleichen soll.

   - **IP-Adresse:** Im Feld *Netzwerke* können Sie Hosts oder Netzwerke hinzufügen oder auswählen, auf die der Filter angewendet werden soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   - **AS-Nummer:** Setzen Sie im Feld *AS-Regex* reguläre BGP-Ausdrücke ein, um AS-Nummern zu definieren, auf die der Filter angewendet werden soll.Beispiel: `_100_` stimmt mit jeder Route durch AS100 überein.

Netzwerke: Fügen Sie Netzwerke und/oder Hosts hinzu, denen Informationen über bestimmte Netzwerke verweigert oder genehmigt werden sollen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Aktion: Wählen Sie aus der Auswahlliste eine Aktion, die ausgeführt werden soll, wenn der Filter zutrifft. Sie können Datenverkehr entweder verweigern oder erlauben.

- **Verwerfen:** Wenn Sie über das Feld *Eingehender Filter* auf der Seite *Neighbor* einem bestimmten Neighbor ein Netzwerk verweigern, ignoriert die UTM Meldungen für dieses Netzwerk. Wenn Sie das Gleiche über das Feld *Ausgehender Filter* durchführen, sendet die UTM für dieses Netzwerk keine Meldungen an den Neighbor.
- **Zulassen:** Wenn Sie über das Feld *Eingehender Filter* auf der Seite *Neighbor* für einen bestimmten Neighbor ein Netzwerk zulassen, empfängt die UTM nur Meldungen für dieses Netzwerk. Wenn Sie das Gleiche über das Feld *Ausgehender Filter* durchführen, sendet die UTM nur für dieses Netzwerk Meldungen an den Neighbor, jedoch für kein anderes Netzwerk, das Sie auf den Seiten *Allgemein* oder *Systeme* definiert haben.

3. **Klicken Sie auf *Speichern*.**
   Die Filterliste wird in der Liste *Filterliste* angezeigt.

Sie können die Filterliste jetzt in einer Neighbor-Definition verwenden.

6.8.6 Erweitert

Auf der Seite *Border Gateway Protocol > Erweitert* können Sie einige zusätzliche Einstellungen für BGP vornehmen und haben Zugriff auf Fenster mit BGP-Informationen zur Fehlersuche.

Mehrere autonome System zulassen

Mehrere AS zulassen: Markieren Sie dieses Auswahlkästchen, falls Sie mehrere AS konfigurieren wollen. Dadurch wird die Seite *Systeme* aktiv, auf der Sie anschließend mehrere AS hinzufügen können. Gleichzeitig wird der Bereich *BGP-System* auf der Seite *Allgemein* deaktiviert und die Seite *Allgemein* zeigt Informationen für alle AS.

Strikte IP-Adressen-Übereinstimmung

Strikte IP-Adressen-Übereinstimmung: Markieren Sie für eine strikte IP-Adressen-Übereinstimmung dieses Auswahlkästchen. Beispiel: 10.0.0.0/8 stimmt nur mit 10.0.0.0/8 überein, aber nicht mit 10.0.1.0/24.

Multi-Pfad-Routing

Normalerweise wird nur eine Route verwendet, selbst wenn es mehrere Routen mit denselben Kosten gibt. Bei Auswahl dieser Option können bis zu acht gleichwertige Routen gleichzeitig verwendet werden. Dies ermöglicht eine Lastverteilung auf mehrere Schnittstellen.

BGP-Fehlersuche

Dieser Abschnitt bietet Zugriff auf drei Fenster mit Informationen für die Fehlersuche. Klicken Sie auf eine Schaltfläche, um ein Fenster zu öffnen. Der Name einer Schaltfläche entspricht dem BGP-Befehl, den Sie normalerweise auf der Kommandozeile eingeben würden. Das Fenster wird dann das Ergebnis dieses Befehls in Form einer Kommandozeilenausgabe anzeigen.

IP-BGP-Neighbor anzeigen: Zeigt Informationen zu den Neighbors der UTM an. Vergewissern Sie sich, dass der Linkstatus jedes Neighbors *Hergestellt* lautet.

IP-BGP-Unicast anzeigen: Zeigt die aktuelle BGP-Routing-Tabelle mit den bevorzugten Pfaden an. Dies ist besonders nützlich, um einen Überblick über Ihre Metrik (metric), Gewichtung (weight) und Präferenz (preference) und deren Auswirkungen zu erhalten.

IP-BGP-Zusammenfassung anzeigen: Zeigt den Status aller BGP-Verbindungen an. Diese Informationen werden auch im Bereich *BGP-Zusammenfassung* auf der Seite *Allgemein* angezeigt.

6.9 Multicast Routing (PIM-SM)

Das Menü *Schnittstellen & Routing > Multicast Routing (PIM-SM)* ermöglicht die Konfiguration von *Protocol Independent Multicast Sparse Mode* (PIM-SM) zur Benutzung in Ihrem Netzwerk. PIM ist ein Protokoll um Multicast-Pakete in Netzwerken dynamisch zu routen. Multicast ist eine Methode, Pakete, die von mehr als einem Client empfangen werden sollen, effizient auszuliefern, indem so wenig Verkehr wie möglich verursacht wird. Normalerweise werden Pakete für mehr als einen Client einfach kopiert und jedem Client individuell zugestellt. Dabei steigt die benötigte Bandbreite mit der Anzahl der Benutzer. Dadurch benötigen Server, die viele Clients haben, die die gleichen Pakete zur gleichen Zeit erfragen, sehr viel Bandbreite, so z. B. Server für Streaming-Inhalte.

Multicast hingegen spart Bandbreite, indem es Pakete nur einmal über jeden Netzwerkknoten sendet. Um das zu erreichen, beteiligt Multicast entsprechend konfigurierte Router an der Entscheidung, wann auf dem Weg vom Server (Absender) zum Client (Empfänger) Kopien erstellt

werden müssen. Die Router benutzen PIM-SM, um die aktiven Multicast-Empfänger im Auge zu behalten, und benutzen diese Information, um das Routen zu konfigurieren.

Ein grobes Schema der PIM-SM-Kommunikation sieht wie folgt aus: Ein Sender beginnt damit, seine Multicast-Daten zu übermitteln. Der Multicast-Router für den Sender registriert sich über PIM-SM am RP-Router, welcher wiederum eine Teilnahmemeldung (join message) an den Router des Senders schickt. Multicast-Pakete fließen nun vom Sender zum RP-Router. Ein Empfänger registriert sich über einen IGMP-Broadcast für diese Multicast-Gruppe bei seinem lokalen PIM-SM-Router. Dieser Router sendet daraufhin eine Teilnahmemeldung für den Empfänger in Richtung RP-Router, welcher im Gegenzug den Multicast-Verkehr an den Empfänger weiterleitet.

Multicast besitzt seinen eigenen IP-Adressbereich: `224.0.0.0/4`.

6.9.1 Allgemein

Auf der Registerkarte *Multicast Routing (PIM-SM) > Allgemein* können Sie PIM aktivieren und deaktivieren. Der Abschnitt *Routing-Daemon-Einstellungen* zeigt den Status der Schnittstellen und beteiligten Router an.

Bevor Sie PIM aktivieren können, müssen Sie zunächst auf der Registerkarte *Schnittstellen* mindestens zwei Schnittstellen definieren, die als PIM-Schnittstellen dienen sollen, und auf der Registerkarte *RP-Router* einen Router.

Um PIM-SM zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie PIM-SM auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Routing-Daemon-Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Aktive PIM-SM-Schnittstellen: Wählen Sie mindestens zwei Schnittstellen für die Benutzung von PIM-SM aus. Schnittstellen können auf der Registerkarte *Schnittstellen* konfiguriert werden.

   Aktive PIM-SM-RP-Router: Wählen Sie mindestens einen RP-Router für die Benutzung von PIM-SM aus. RP-Router können auf der Registerkarte *RP-Router* definiert werden.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert. PIM-SM-Kommunikation in Ihrem Netzwerk ist nun aktiviert.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler. Um PIM-SM zu deaktivieren, klicken Sie auf den grünen Schieberegler.

Live-Protokoll

Klicken Sie auf *Live-Protokoll öffnen*, um das PIM-Live-Protokoll in einem neuen Fenster zu öffnen.

6.9.2 Schnittstellen

Auf der Registerkarte *Multicast Routing (PIM-SM) > Schnittstellen* können Sie festlegen, über welche Schnittstellen von Sophos UTM Multicast-Kommunikation stattfinden soll.

Um eine neue PIM-SM-Schnittstelle anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue PIM-SM-Schnittstelle*.**
   Das Dialogfeld *Neue PIM-SM-Schnittstelle anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die PIM-SM-Schnittstelle ein.

   Schnittstelle: Wählen Sie eine Schnittstelle aus, die PIM- und IGMP-Netzwerkverkehr annehmen soll.

   DR-Priorität (optional): Geben Sie eine Zahl ein, die die designierte Router-Priorität (DR) für diese Schnittstelle festlegt. Der Router mit der höchsten Zahl nimmt IGMP-Anfragen an, wenn mehr als ein PIM-SM-Router im selben Netzwerksegment präsent ist. Zahlen von `0` bis 2^{32} sind erlaubt. Wenn Sie keine Priorität angeben, wird der Wert `0` gesetzt.

   IGMP: Wählen Sie die Version des *Internet-Group-Management-Protokolls* (Internet Group Management Protocol), die unterstützt werden soll. IGMP wird von Empfängern benutzt, um einer Multicast-Gruppe beizutreten.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue PIM-SM-Schnittstelle wird zur Schnittstellenliste hinzugefügt.

Um eine PIM-SM-Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.9.3 RP-Router

Um Multicast in Ihrem Netzwerk verwenden zu können, müssen Sie einen oder mehrere Rendezvous-Point-Router (RP-Router) konfigurieren. Ein RP-Router nimmt Registrierungen sowohl von Multicast-Empfängern als auch Multicast-Sendern an.Ein RP-Router ist ein regulärer PIM-SM-Router, der dazu auserkoren wurde, außerdem als RP-Router für bestimmte Multicast-Gruppen zu agieren. Alle PIM-SM-Router müssen darin übereinstimmen, welcher Router der RP-Router ist.

Um einen RP-Router anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *RP-Router* auf *Neuer Rendezvous-Point-Router*.**
   Das Dialogfeld *Neuen RP-Router anlegen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den RP-Router ein.

   Host: Legen Sie einen Host an (oder wählen Sie einen aus), der als Rendezvous-Point-Router agieren soll.

   Priorität: Geben Sie eine Zahl an, die die Priorität des RP-Routers festlegt. Teilnahmemeldungen werden zu dem RP-Router mit der niedrigsten Priorität gesendet. Zahlen von `0` bis `255` sind erlaubt. Wenn Sie keine Priorität angeben, wird der Wert `0` gesetzt.

   Multicast-Gruppenpräfixe: Geben Sie die Multicast-Gruppe ein, für die der RP-Router verantwortlich ist. Sie können Gruppenpräfixe wie `224.1.1.0/24` festlegen, falls der RP für mehr als eine Multicast-Gruppe verantwortlich ist. Die Multicast-Gruppe oder das Gruppenpräfix muss sich innerhalb des Multicast-Adressbereichs befinden, der `224.0.0.0/4` ist.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.
3. **Klicken Sie auf *Speichern*.**
   Der neue RP-Router wird in der Routerliste angezeigt.

Um einen RP-Router zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.9.4 Routen

Sie müssen zwischen Sender(n) und Empfängern eine durchgängige Kommunikationsroute einrichten. Wenn Empfänger, Sender und/oder RP-Router sich nicht im selben Netzwerksegment befinden, werden Sie eine Route anlegen müssen, um die Kommunikation zwischen ihnen zu gewährleisten.

Um eine PIM-SM-Route anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Routen* auf *Neue PIM-SM-Route*.**
   Das Dialogfeld *Neue PIM-SM-Route anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

   Routentyp: Die folgenden Routentypen sind verfügbar:

   - **Schnittstellen-Route:** Datenpakete werden an eine bestimmte Schnittstelle geschickt. Dieser Typ kann in zwei Fällen nützlich sein: Für Routing-Einträge zu dynamischen Schnittstellen (z. B. PPP), da in diesem Fall die IP-Adresse des Gateways nicht bekannt ist, oder für eine Standard-Route mit einem Gateway außerhalb der direkt angeschlossenen Netzwerke.
   - **Gateway-Route:** Die Datenpakete werden an einen bestimmten Host (Gateway) geschickt.

   Netzwerk: Wählen Sie den Zieladressbereich aus, wohin der PIM-Verkehr geroutet werden soll.

   Gateway: Wählen Sie das Gateway/den Router aus, an das oder den das Gateway die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Gateway-Route* als Routentyp gewählt haben).

   Schnittstelle: Wählen Sie die Schnittstelle aus, zu der das Gateway die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Schnittstellenroute* als Routentyp ausgewählt haben).

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue PIM-SM-Route wird zur Routenliste hinzugefügt.

Um eine PIM-SM-Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

6.9.5 Erweitert

Auf der Registerkarte *Schnittstellen & Routing > Multicast Routing (PIM-SM) > Erweitert* können Sie erweiterte Einstellungen für PIM konfigurieren.

Shortest-Path-Tree-Einstellungen

In einigen Netzwerken ist die PIM-Kommunikationsroute zwischen Sender, RP und Empfänger nicht der kürzestmögliche Netzwerkpfad. Die Option *Wechsel zu Shortest-Path-Tree ermöglichen* erlaubt es, eine bestehende Kommunikation zwischen Sender und Empfänger auf den kürzestmöglichen verfügbaren Pfad zu verlegen, wenn ein gewisser Schwellenwert erreicht ist, wobei der RP dann als Vermittler ausgelassen wird.

Automatische Firewalleinstellungen

Wenn Sie diese Option auswählen, wird das System automatisch alle notwendigen Firewallregeln anlegen, die benötigt werden, um Multicast-Verkehr für die angegebenen Multicast-Gruppen weiterzuleiten.

Fehlersuche-Einstellungen

Wählen Sie die Option *Fehlersuche-Modus aktivieren*, um zusätzliche Informationen für die Fehlersuche im PIM-SM Routing-Daemon-Protokoll anzuzeigen.

7 Netzwerkdienste

In diesem Kapitel wird die Konfiguration verschiedener Netzwerkdienste von Sophos UTM für Ihr Netzwerk beschrieben.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- DNS
- DHCP
- NTP

7.1 DNS

Die Registerkarten des Menüs *Netzwerkdienste* > *DNS* enthalten eine Reihe von Konfigurationsmöglichkeiten, die sich auf den Dienst *Domain Name System* (DNS) beziehen. Die Hauptaufgabe von DNS ist die Übersetzung von Domänennamen (Hostnamen) in die zugehörigen IP-Adressen.

7.1.1 Allgemein

Zugelassene Netzwerke

Sie können die Netzwerke angeben, die UTM für die rekursive DNS-Auflösung nutzen können sollen. Üblicherweise wird dies nur den internen Netzwerken (LAN) gestattet.

Warnung – Wählen Sie niemals das Netzwerkobjekt *Any* aus, weil Sie dadurch Ihre Appliance einem hohen Risiko für Angriffe aus dem Internet aussetzen würden.

Hinweis – Wenn Sie bereits einen internen DNS-Server nutzen, z. B. in Verbindung mit Active Directory, sollten Sie dieses Feld leer lassen.

DNSSEC

Die Domain Name System Security Extensions (DNSSEC) sind Erweiterungen für DNS, die die Sicherheit verbessern. DNSSEC versieht die DNS-Lookup-Einträge mit Hilfe von Public-Key-Kryptografie mit einer digitalen Signatur. Ist die Option nicht ausgewählt, akzeptiert die

UTM alle DNS-Einträge. Ist die Option ausgewählt, validiert die UTM eingehende DNS-Anfragen bezüglich ihrer DNSSEC-Signierung. Aus den signierten Zonen werden nur korrekt signierte Einträge akzeptiert.

Hinweis – Wenn die Option ausgewählt ist, kann es passieren, dass DNS-Einträge von manuell installierten oder vom ISP zugewiesenen Forwarders abgelehnt werden, die nicht DNSSEC-fähig sind. Entfernen Sie in diesem Fall auf der Registerkarte *Weiterleitung* die DNS-Forwarders aus dem Feld und/oder deaktivieren Sie das Kontrollkästchen *Vom ISP zugewiesene Forwarders verwenden*.

DNS-Speicher leeren

Der DNS-Proxy benutzt einen Zwischenspeicher (Cache) für seine Einträge. Jeder Eintrag hat ein Ablaufdatum (TTL, Time-To-Live), an dem er gelöscht wird. Die TTL beträgt normalerweise einen Tag. Sie können den Cache jedoch manuell leeren, wenn Sie z. B. wollen, dass jüngste Änderungen in DNS-Einträgen sofort berücksichtigt werden, ohne darauf warten zu müssen, dass die TTL abläuft. Um den Cache zu leeren, klicken Sie auf *DNS-Speicher jetzt leeren*.

7.1.2 Weiterleitung

Auf der Registerkarte *Netzwerkdienste > DNS > Weiterleitung* können Sie sogenannte DNS-Forwarders (Weiterleitungen) spezifizieren. Ein DNS-Forwarder ist ein *Domain-Name-System*-Server (DNS), der DNS-Anfragen für externe DNS-Namen an DNS-Server außerhalb des Netzwerks weiterleitet. Fügen Sie Ihrer Konfiguration wenn möglich einen DNS-Forwarder hinzu. Dies sollte ein lokaler Host oder idealerweise ein Server sein, der von Ihrem Internetanbieter (ISP) betrieben wird. Dieser wird dann als übergeordneter Zwischenspeicher verwendet und Ihre DNS-Anfragen deutlich beschleunigen. Wenn Sie keinen Namensserver für die Weiterleitung angeben, werden stattdessen die Root-DNS-Server gefragt, die zunächst einmal Zoneninformationen einholen und deshalb eine längere Beantwortungszeit benötigen.

Um einen DNS-Forwarder anzulegen, gehen Sie folgendermaßen vor:

1. **Wählen Sie einen DNS-Forwarder aus.**
   Wählen Sie einen DNS-Forwarder aus oder fügen Sie einen hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Vom ISP zugewiesene Forwarders verwenden (optional): Wählen Sie die Option *Vom ISP zugewiesene Forwarders verwenden*, um DNS-Anfragen an DNS-Server Ihres ISP weiterzuleiten. Wenn diese Option ausgewählt ist, werden alle Forwarders, die automatisch von Ihrem ISP zugewiesen werden, in der Zeile unter dem Feld aufgelistet.

2. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

7.1.3 Anfragerouten

Angenommen, Sie betreiben Ihren eigenen internen DNS-Server. Dann kann dieser Server dazu verwendet werden, als alternativer Server DNS-Anfragen für Domänen aufzulösen, die Sie nicht von DNS-Forwarders auflösen lassen wollen. Auf der Registerkarte *Netzwerkdienste > DNS > Anfragerouten* können Sie Routen zu eigenen DNS-Servern definieren.

Um eine DNS-Anfrageroute anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Anfragerouten* auf *Neue DNS-Anfrageroute*.**
   Das Dialogfeld *Neue DNS-Anfrageroute erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Domäne: Tragen Sie die Domäne ein, für die ein alternativer DNS-Server genutzt werden soll.

   Zielserver: Wählen Sie einen oder mehrere DNS-Server für die Auflösung der oben angegebenen Domäne aus oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Route wird in der Liste *DNS-Anfragerouten* angezeigt und ist sofort aktiv.

Um eine DNS-Anfrageroute zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

7.1.4 Statische Einträge

Wenn Sie keinen eigenen DNS-Server einrichten wollen, aber eine statische DNS-Zuordnung für einige Hosts benötigen, können Sie diese Zuordnungen anlegen.

Ab UTM Version 9.1 befindet sich diese Funktion auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*. Die DNS-Zuordnungen werden nun zusammen mit den beteiligten Hosts definiert.

Wenn Sie auf die Schaltfläche *Statische Einträge* klicken, öffnet sich die Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*. Automatisch werden nur Hosts mit statischen Einträgen angezeigt. Verwenden Sie die Auswahlliste oberhalb der Liste, um die Filtereinstellungen zu ändern.

7.1.5 DynDNS

Dynamic DNS oder kurz DynDNS ist ein Domänennamensdienst, der es ermöglicht, statische Internetdomänennamen einem Computer mit variabler IP-Adresse zuzuordnen. Sie können sich für DynDNS auf der Website des jeweiligen DynDNS-Anbieters anmelden, um einen DNS-Alias anzufordern, der automatisch aktualisiert wird, wenn sich Ihre Uplink-IP-Adresse ändert. Wenn Sie sich bei diesem Dienst registriert haben, erhalten Sie einen Hostnamen, einen Benutzernamen und ein Kennwort, welche für die Konfiguration benötigt werden.

Um DynDNS zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *DynDNS* auf *Neue DynDNS*.**
   Das Dialogfeld *Neues DynDNS erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Art: Die folgenden DynDNS-Dienste sind verfügbar:

   - **DNSdynamic:** Offizielle Website: www.dnsdynamic.org
   - **DNS Park:** Offizielle Website: www.dnspark.com
   - **DtDNS:** Offizielle Website: www.dtdns.com
   - **DynDNS:** Standardmäßiger DNS-Dienst des Dienstanbieter Dynamic Network Services Inc. (Dyn). Offizielle Website: www.dyndns.com

- **Custom DynDNS:** Benutzerdefinierter DNS-Dienst des Dienstanbieter Dynamic Network Services Inc.(Dyn) (www.dyndns.com). Dieser Dienst ist hauptsächlich für Benutzer, die ihre Domäne selbst besitzen oder selbst registriert haben.
- **easyDNS:** Offizielle Website: www.easydns.com
- **FreeDNS:** Offizielle Website: freedns.afraid.org
- **Namecheap:** Offizielle Website: www.namecheap.com
- **No-IP.com:** Offizielle Website: www.noip.com
- **OpenDNS-IP-Update:** Offizielle Website: www.opendns.com
- **selfHOST:** Offizielle Website: www.selfhost.de
- **STRATO AG:** Offizielle Website: www.strato.de
- **zoneedit:** Offizielle Website: www.zoneedit.com

Hinweis – Im Feld *Server* wird die URL angezeigt, an welche die UTM die IP-Änderungen sendet.

Zuweisen (nicht beim Typ *FreeDNS*): Legen Sie die IP-Adresse fest, der der DynDNS-Name zugeordnet wird. Wählen Sie *IP der lokalen Schnittstelle*, wenn die betreffende Schnittstelle eine öffentliche IP-Adresse hat. Üblicherweise werden Sie diese Option für Ihre DSL-Internetverbindung verwenden. Bei der Option *Erste öffentliche IP auf der Standardroute* müssen keine Schnittstellen spezifiziert werden. Die UTM sendet stattdessen eine WWW-Anfrage zu einem öffentlichen DynDNS-Server, der im Gegenzug mit der öffentlichen IP-Adresse antwortet, die Sie gerade verwenden. Dies ist hilfreich, wenn die UTM über keine öffentliche IP-Adresse verfügt, sondern sich in einem privaten Netzwerk befindet und sich über einen maskierenden Router mit dem Internet verbindet.

Hinweis – FreeDNS verwendet immer die erste öffentliche IP-Adresse auf der Standardroute.

Schnittstelle (nicht bei Typ *FreeDNS*, nur bei *IP der lokalen Schnittstelle*): Wählen Sie die Schnittstelle, für die Sie den DynDNS-Dienst verwenden möchten. Wahrscheinlich wird es sich dabei um Ihre externe Schnittstelle handeln, die mit dem Internet verbunden ist.

Hostname (nicht bei Typ *Open-DNS-IP-Update*):Tragen Sie die Domäne ein, die Sie von Ihrem DynDNS-Anbieter erhalten haben (z. B. `example.dyndns.org`). Sie müssen sich für den Hostnamen an keine spezielle Syntax einhalten. Das, was Sie hier eingeben müssen, hängt ausschließlich davon ab, was Ihr DynDNS-Dienstanbieter erfordert. Überdies können Sie optional Ihren DynDNS-Hostnamen auch als den Haupthostnamen für Ihr Gateway verwenden.

Bezeichnung (nur beim Typ *Open-DNS-IP-Update*): Geben Sie die Bezeichnung des Netzwerks ein. Weitere Informationen finden Sie in der Wissensdatenbank von OpenDNS.

Aliasse (optional, nur bei manchen Typen): In dieses Dialogfenster können zusätzliche Hostnamen eingetragen werden, die auf dieselbe IP-Adresse verweisen wie der Haupthostname oben (z. B. `mail.beispiel.de, beispiel.de`).

MX (optional, nur beim Typ *DNS Park*, *DynDNS* oder *easyDNS*): Mail-Exchange-Server werden dazu benutzt, E-Mails an bestimmte Server umzuleiten, auf welche der Hostname nicht verweist. MX-Einträge (engl. MX records) ermöglichen, dass E-Mails an eine bestimmte Domäne zu einem bestimmten Host (Server) geleitet werden.Beispiel: Wenn im Eingabefeld als Mail-Exchange-Server `mail.beispiel.de` eingetragen ist, dann wird eine E-Mail mit der Adresse `benutzer@beispiel.de` an den Host `mail.beispiel.de` gesendet.

MX-Priorität (optional, nur beim Typ *DNS Park*): Geben Sie eine positive Ganzzahl ein, die angibt, ob der angegebene Mail-Server bei der Zustellung der E-Mail gegenüber der Domäne bevorzugt werden sollte. Server mit niedrigeren Zahlen erhalten den Vorzug gegenüber Servern mit höheren Zahlen. Normalerweise können Sie dieses Feld leer lassen, da DNS Park den Standardwert 5 verwendet, der für fast jeden Fall geeignet ist.Technische Details zu den Mail-Exchanger-Prioritäten finden Sie unter RFC 5321.

Backup-MX (optional, nur beim Typ *DynDNS* oder *easyDNS*): Wählen Sie diese Option nur aus, wenn der Hostname im Feld *Hostname* als Hauptmailserver dienen soll. Dann wird der Hostname im Feld *MX* nur als Backup-Mailserver eingesetzt.

Platzhalter (optional, nur beim Typ *DynDNS* oder *easyDNS*): Wählen Sie diese Option, wenn die Subdomänen auf die gleiche IP-Adresse wie Ihre registrierte Domäne verweisen sollen. Bei Verwendung dieser Option wird Ihrer Domäne ein Asterisk (*) beigefügt, der als Platzhalter dient (z. B. `*.beispiel.dyndns.org`). Das stellt sicher, dass z. B. `www.beispiel.dyndns.org` auf dieselbe Adresse verweist wie `beispiel.dyndns.org`.

Benutzername: Tragen Sie den Benutzernamen ein, den Sie vom DynDNS-Anbieter erhalten haben.

Kennwort: Tragen Sie das Kennwort ein, das Sie vom DynDNS-Anbieter erhalten haben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Das neue DynDNS wird in der Liste *DynDNS* angezeigt. Der Dienst ist noch deaktiviert (Schieberegler ist grau).

4. **Aktivieren Sie DynDNS.**
   Klicken Sie auf den Schieberegler, um den DynDNS-Dienst zu aktivieren.

   Der Dienst ist jetzt aktiv (Schieberegler ist grün).

Um ein DynDNS zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Sie können mehrere DynDNS-Einträge gleichzeitig verwenden. Wenn alle Einstellungen für zwei Hostnamen identisch sind, empfiehlt es sich, die Option *Aliasse* zu verwenden, anstatt zwei Einzeleinträge anzulegen.

7.2 DHCP

Das *Dynamic Host Configuration Protocol* (DHCP, dynamisches Hostkonfigurationsprotokoll) verteilt automatisch Adressen aus einem festgelegten IP-Adressbereich an angeschlossene Clients. Dies spart bei größeren Netzwerken viel Konfigurationsaufwand und beugt Adressenkonflikten vor. Das DHCP verteilt IP-Adressen, Standardgateway-Informationen und DNS-Konfigurationsdaten an seine Clients.

Zusätzlich zur vereinfachten Konfiguration von Clientrechnern und zum problemlosen Wechseln von mobilen Computern zwischen verschiedenen Netzwerken lassen sich in einem DHCP-Netzwerk Fehler einfacher lokalisieren und beheben, da die Konfiguration der IP-Adressen primär von den Einstellungen des DHCP-Servers abhängen. Außerdem lassen sich Adressbereiche effektiver nutzen, vor allem, wenn nicht alle Rechner gleichzeitig im Netzwerk aktiv sind. Die IP-Adressen können so je nach Bedarf vergeben und wiederverwendet werden.

7.2.1 Server

Auf der Registerkarte *Netzwerkdienste > DHCP > Server* können Sie einen DHCP-Server konfigurieren. Sophos UTMstellt den DHCP-Dienst für das angeschlossene Netzwerk sowie für weitere Netzwerke bereit. Der DHCP-Server kann dazu verwendet werden, Ihren Clients grundlegende Netzwerkparameter zuzuweisen. Sie können den DHCP-Dienst auf verschiedenen Schnittstellen laufen lassen, wobei jede Schnittstelle und jedes bereitzustellende Netzwerk individuell konfiguriert werden können.

Hinweis – Auf der Registerkarte *Optionen* können Sie zusätzliche oder andere DHCP-Optionen definieren, die an die Clients gesendet werden. Eine DHCP-Option, die auf der Registerkarte *Optionen* definiert ist, überschreibt eine Einstellung auf der Registerkarte *Server*, wenn ihr Geltungsbereich nicht allgemein ist. Wenn Sie DHCP-Optionen nur für ausgewählte Hosts definieren, können Sie ihnen einen DNS-Server oder eine Lease-Zeit zuweisen, die von der Definition für den DHCP-Server abweichen kann.

Um einen DHCP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer DHCP-Server*.**
   Das Dialogfeld *Neuen DHCP-Server erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Schnittstelle: Wählen Sie die Schnittstelle aus, von der aus den Clients die IP-Adressen zugewiesen werden. Es kann nur eine bereits konfigurierte Schnittstelle ausgewählt werden.

   Adresstyp: Diese Option ist nur verfügbar, wenn IPv6 global aktiviert ist. Wählen Sie die IP-Version des DHCP-Servers.

   Bereichsbeginn/-ende: Der IP-Adressbereich, der als Kontingent für diese Schnittstelle verwendet wird. Standardmäßig ist der konfigurierte Adressbereich der Netzwerkkarte eingestellt. Wenn sich die Clients im gleichen Netzwerk befinden, muss sich der Bereich innerhalb des Netzwerks befinden, das mit der Schnittstelle verbunden ist. Wenn sich die Clients in einem anderen Netzwerk befinden, muss sich der Bereich innerhalb desjenigen Netzwerks befinden, aus dem die Relay-DHCP-Anfragen weitergeleitet werden.

> **Hinweis –** Je größer der definierte DHCP-IP-Bereich ist, desto mehr Speicher reserviert die UTM dafür. Reduzieren Sie daher den DHCP-Bereich auf die Werte, die Sie tatsächlich benötigen. Der größte erlaubte Bereich ist ein /9-Netzwerk.

DNS-Server 1/2: Die IP-Adressen der DNS-Server.

Standardgateway (nur bei IPv4): Die IP-Adresse des Standardgateways.

> **Hinweis –** Sowohl für WLAN-Access-Points als auch für RED-Appliances muss sich das Standardgateway im selben Subnetz befinden wie die Schnittstelle, an die diese Appliances angeschlossen sind.

Domäne (optional): Tragen Sie den Domänennamen ein, der an die Clients übermittelt werden soll (z. B. `intranet.beispiel.de`).

Lease-Zeit (nur bei IPv4): Der DHCP-Client versucht, den Lease automatisch zu erneuern. Wenn der Lease während der Lease-Zeit nicht erneuert wird, läuft der Lease der IP-Adresse ab. Hier können Sie diesen Zeitraum in Sekunden festlegen. Der Standard ist 86.400 Sekunden (ein Tag). Das Minimum beträgt 600 Sekunden (10 Minuten) und das Maximum beträgt 2.592.000 Sekunden (ein Monat).

Gültige Lebensdauer (nur bei IPv6): Der DHCP-Client versucht, den Lease automatisch zu erneuern. Wenn der Lease während seiner gültigen Lebensdauer nicht erneuert wird, wird der Lease-Status der IP-Adresse ungültig, die Adresse wird von der Schnittstelle entfernt und kann anderweitig zugewiesen werden. Sie können ein Intervall zwischen fünf Minuten und unendlich auswählen. Die gültige Lebensdauer muss jedoch mindestens der bevorzugten Lebensdauer entsprechen.

Bevorzugte Lebensdauer (nur bei IPv6): Der DHCP-Client versucht, den Lease automatisch zu erneuern. Wenn der Lease während seiner gültigen Lebensdauer nicht erneuert wird, wird der Lease-Status der IP-Adresse überholt, d.h. er ist zwar noch gültig, wird jedoch nicht für neue Verbindungen verwendet. Sie können ein Intervall zwischen fünf Minuten und unendlich auswählen.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**

WINS-Knotentyp (nur bei IPv4): *Windows Internet Naming Service* (WINS, Windows-Internet-Namensdienst) ist Microsofts Implementierung des *NetBIOS Name Server* (NBNS) für Windows-Betriebssysteme. Dabei handelt es sich um einen Namensserver

und -dienst für NetBIOS-Computernamen. Ein WINS-Server verhält sich wie eine Datenbank, die Hostnamen mit IP-Adressen vergleicht. Dadurch ermöglicht er Computern, die NetBIOS verwenden, das TCP/IP-Protokoll zu nutzen. Die folgenden WINS-Knotentypen sind verfügbar:

- **Nicht festlegen:** Der WINS-Knotentyp ist nicht festgelegt und wird vom Client selbst bestimmt.
- **B-Knoten (kein WINS):** B-Knotensysteme verwenden ausschließlich Broadcast.
- **P-Knoten (nur WINS):** P-Knotensysteme verwenden nur Punkt-zu-Punkt-Namensanfragen für einen Windows-Namensserver (WINS).
- **M-Knoten (Broadcast, dann WINS):** Bei M-Knotensystemen erfolgt zuerst ein Broadcast, dann wird der Namensserver angefragt.
- **H-Knoten (WINS, dann Broadcast):** Bei H-Knotensystemen wird zuerst der Namensserver angefragt, dann erfolgt ein Broadcast.

WINS-Server: Je nach gewähltem WINS-Knotentyp erscheint dieses Textfeld. Geben Sie hier die IP-Adresse des WINS-Servers ein.

Nur Clients mit statischer Zuordnung (optional): Wählen Sie diese Option aus, damit der DHCP-Server IP-Adressen nur an Clients vergibt, die eine statische DHCP-Zuordnung besitzen (siehe *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen*).

HTTP-Proxy-Autokonfiguration aktivieren: Wählen Sie diese Option, wenn Sie eine PAC-Datei für die automatische Proxy-Konfiguration von Browsern bereitstellen wollen. Weitere Informationen finden Sie im Kapitel *Web Protection > Filteroptionen > Sonstiges*, Abschnitt *Automatische Proxy-Konfiguration*.

Hinweis – Die automatische HTTP-Proxy-Konfiguration wird derzeit bei IPv6 nicht von Microsoft Windows unterstützt.

Clients über DHCP-Relay-Agent: Bei Auswahl dieser Option weist der DHCP-Server Clients, die sich nicht im Netzwerk der verbundenen Schnittstelle befinden, IP-Adressen zu. In diesem Fall muss sich der oben definierte Adressbereich in dem Netzwerk befinden, aus dem Relay-DHCP-Anfragen weitergeleitet werden, und nicht im Netzwerk der verbundenen Schnittstelle.

Netzmaske: Wählen Sie die Netzmaske des Netzwerks aus, aus dem die Relay-DHCP-Anfragen weitergeleitet werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

4. **Klicken Sie auf *Speichern*.**
   Die neue DHCP-Serverdefinition wird in der DHCP-Server-Liste angezeigt und ist sofort aktiv.

Um eine DHCP-Serverdefinition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

7.2.2 Relay

Auf der Registerkarte *Netzwerkdienste > DHCP > Relay* können Sie ein DHCP-Relay konfigurieren. Der DHCP-Dienst wird von einem separaten DHCP-Server bereitgestellt und die UTM fungiert als Relay. Das DHCP-Relay kann zur Weiterleitung von DHCP-Anfragen und -Antworten über verschiedene Netzwerksegmente hinweg verwendet werden. Bevor die Einstellungen für das DHCP-Relay durchgeführt werden können, muss der separate DHCP-Server konfiguriert sein.

Um ein DHCP-Relay zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Relay* die Option *DHCP-Relay*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *DHCP-Relaykonfiguration* kann nun bearbeitet werden.

2. **Wählen Sie den DHCP-Server aus.**

3. **Wählen Sie die beteiligten Schnittstellen aus.**
   Fügen Sie sowohl die Schnittstelle zum DHCP-Server als auch die Schnittstellen zu den Client-Netzwerken hinzu, zwischen denen DHCP-Anfragen und -Antworten weitergeleitet werden.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

7.2.3 Statische Zuordnungen

Sie können statische Zuordnungen zwischen Clients und IP-Adressen für einige oder alle Clients erstellen. Ab UTM Version 9.1 befindet sich diese Funktion auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*. Die DHCP-Zuordnungen werden nun zusammen mit den beteiligten Hosts definiert.

Wenn Sie auf die Schaltfläche *Statische Zuordnungen* klicken, öffnet sich die Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*. Automatisch werden nur Hosts mit statischen Zuordnungen angezeigt. Verwenden Sie die Auswahlliste oberhalb der Liste, um die Filtereinstellungen zu ändern.

7.2.4 IPv4-Lease-Tabelle

Wenn der DHCP-Dienst genutzt wird, besitzt ein Client keine eigene IP-Adresse mehr, sondern *least* diese vom DHCP-Server. Dieser erteilt dem Client die Berechtigung, die IP-Adresse für einen gewissen Zeitraum zu verwenden.

Die Lease-Tabelle auf der Registerkarte *Netzwerkdienste > DHCP > IPv4-Lease-Tabelle* zeigt die aktuellen IP-Adresszuweisungen des DHCP-Servers, einschließlich Informationen über den Beginn der Zuweisung und die Ablaufzeit der IP-Adresse.

Statische Zuordnung für eine neue Hostdefinition hinzufügen

Sie können einen bestehenden Lease als Vorlage für eine statische MAC/IP-Zuordnung mit einem zu definierenden Host verwenden. Gehen Sie folgendermaßen vor:

1. **Klicken Sie für den gewünschten Lease in der Spalte *Statisch machen* auf *Statisch machen*.**
   Das Dialogfenster *Statisch machen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Aktion: Wählen Sie *Neuen Host anlegen*.

   Name: Geben Sie einen aussagekräftigen Namen für den neuen Host ein.

   DHCP-Server: Wählen Sie den DHCP-Server aus, der für die statische Zuordnung verwendet werden soll. Der entsprechende DHCP-Bereich wird unter der Auswahlliste angezeigt.

IPv4-Adresse: Ändern Sie die IP-Adresse auf eine Adresse außerhalb des DHCP-Pool-Bereichs.

> **Hinweis –** Wenn ein Lease in eine statische Zuordnung umgewandelt wird, sollten Sie die IP-Adresse ändern, sodass sie nicht mehr im DHCP-Pool-Bereich liegt. Wenn Sie die IP-Adresse ändern, ändert sich die IP-Adresse des Clients jedoch nicht sofort, sondern erst dann, wenn er das nächste Mal versucht, seinen Lease zu erneuern.

DNS-Hostname: Wenn Sie einen DNS-Hostnamen eingeben, wird dieser als statischer DNS-Eintrag für den Host verwendet.

Reverse-DNS: Markieren Sie dieses Auswahlkästchen, um die Zuordnung der IP-Adresse des Hosts zu seinem Namen zu ermöglichen. Beachten Sie, dass eine IP-Adresse immer nur auf einen Namen verweisen kann, wohingegen mehrere Namen auf die gleiche IP-Adresse verweisen können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

Den neuen Host mit der statischen Zuordnung finden Sie auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*.

Statische Zuordnung für eine vorhandene Hostdefinition hinzufügen

Sie können eine bestehende IP-Adresszuweisung für eine statische MAC/IP-Zuordnung einer vorhandenen Hostdefinition verwenden. Gehen Sie folgendermaßen vor:

1. **Klicken Sie für die gewünschte IP-Adresszuweisung in der Spalte *Statisch machen* auf *Statisch machen*.**
   Das Dialogfenster *Statisch machen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Aktion: Wählen Sie *Vorhandenen Host verwenden*.

   Host: Fügen Sie den Host hinzu, indem Sie auf das Ordnersymbol klicken.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

Den Host mit der statischen Zuordnung finden Sie auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*.

7.2.5 IPv6-Lease-Tabelle

Wenn der DHCP-Dienst genutzt wird, besitzt ein Client keine eigene IP-Adresse mehr, sondern *least* diese vom DHCP-Server. Dieser erteilt dem Client die Berechtigung, die IP-Adresse für einen gewissen Zeitraum zu verwenden.

Die Lease-Tabelle auf der Registerkarte *Netzwerkdienste > DHCP > IPv6-Lease-Tabelle* zeigt die aktuellen Leases des DHCP-Servers, einschließlich Informationen über den Beginn und die Ablaufzeit des Leases.

Hinweis – Leases, die über Präfix-Bekanntmachungen vergeben wurden, werden in der Tabelle nicht aufgeführt.

Statische Zuordnung für eine neue Hostdefinition hinzufügen

Sie können einen bestehenden Lease als Vorlage für eine statische MAC/IP-Zuordnung mit einem zu definierenden Host verwenden. Gehen Sie folgendermaßen vor:

1. **Klicken Sie für den gewünschten Lease auf *Statisch machen*.**
   Das Dialogfenster *Statisch machen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Aktion: Wählen Sie *Neuen Host anlegen*.

   Name: Geben Sie einen aussagekräftigen Namen für den neuen Host ein.

   DHCP-Server: Wählen Sie den DHCP-Server aus, der für die statische Zuordnung verwendet werden soll. Der entsprechende DHCP-Bereich wird unter der Auswahlliste angezeigt.

   IPv6-Adresse: Ändern Sie die IP-Adresse auf eine Adresse außerhalb des DHCP-Pool-Bereichs.

   Hinweis – Wenn ein Lease in eine statische Zuordnung umgewandelt wird, sollten Sie die IP-Adresse ändern, sodass sie nicht mehr im DHCP-Pool-Bereich liegt. Wenn Sie die IP-Adresse ändern, ändert sich die IP-Adresse des Clients jedoch nicht sofort, sondern erst dann, wenn er das nächste Mal versucht, seinen Lease zu erneuern.

DNS-Hostname: Wenn Sie einen DNS-Hostnamen eingeben, wird dieser als statischer DNS-Eintrag für den Host verwendet.

Reverse-DNS: Markieren Sie dieses Auswahlkästchen, um die Zuordnung der IP-Adresse des Hosts zu seinem Namen zu ermöglichen. Beachten Sie, dass eine IP-Adresse immer nur auf einen Namen verweisen kann, wohingegen mehrere Namen auf die gleiche IP-Adresse verweisen können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

Statische Zuordnung für eine vorhandene Hostdefinition hinzufügen

Sie können eine bestehende IP-Adresszuweisung für eine statische MAC/IP-Zuordnung einer vorhandenen Hostdefinition verwenden. Gehen Sie folgendermaßen vor:

1. **Klicken Sie für die gewünschte IP-Adresszuweisung in der Spalte *Statisch machen* auf *Statisch machen*.**
   Das Dialogfenster *Statisch machen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Aktion: Wählen Sie *Vorhandenen Host verwenden*.

   Host: Fügen Sie den Host hinzu, indem Sie auf das Ordnersymbol klicken.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

Den Host mit der statischen Zuordnung finden Sie auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen*.

7.2.6 Optionen

Auf der Registerkarte *Netzwerkdienste > DHCP > Optionen* können Sie DHCP-Optionen konfigurieren. DHCP-Optionen sind zusätzliche Konfigurationsparameter, die DHCP-Clients von einem DHCP-Server zur Verfügung gestellt werden.

Beispiel: Um einigen VoIP-Telefonen die erforderlichen Informationen von Ihren DHCP-Servern bereitzustellen, müssen Sie auf dieser Seite drei zusätzliche DHCP-Optionen erstellen und aktivieren:

- *filename*: Name der Boot-Datei.
- *next-server*: Name des TFTP-Servers, der die Boot-Datei bereitstellt.
- *4 (Zeitserver)*: IP-Adresse des Zeitservers.

DHCP-Optionen können unterschiedliche Geltungsbereiche aufweisen: Sie können beispielsweise nur ausgewählten Hosts, nur von ausgewählten Servern oder sogar global bereitgestellt werden. Daher ist es möglich, für denselben Host unterschiedliche Parameter zu definieren. Einige DHCP-Optionen sind bereits auf der Registerkarte *DHCP > Server* festgelegt, z. B. DNS-Server (Option 6). Im Falle von widersprüchlichen Parameterwerten werden die Parameter dem Client gemäß folgender Prioritäten bereitgestellt:

1. DHCP-Option mit Geltungsbereich *Host*
2. DHCP-Option mit Geltungsbereich *MAC-Präfix*
3. DHCP-Option mit Geltungsbereich *Anbieter-ID*
4. DHCP-Option mit Geltungsbereich *Server*
5. DHCP-Serverparameter (Registerkarte *DHCP > Server*)
6. DHCP-Option mit Geltungsbereich *Allgemein*

Hinweis – Mit der DHCP-Anfrage übermittelt ein DHCP-Client die Informationen darüber, welche DHCP-Optionen er verarbeiten kann. Daraufhin stellt der DHCP-Server nur die DHCP-Optionen bereit, die der Client versteht, unabhängig davon, welche Optionen hier definiert sind.

Um eine DHCP-Option anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Neue DHCP-Option*.**
   Das Dialogfeld *Neue DHCP-Option erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Adresstyp (nur, wenn IPv6 aktiviert ist): Wählen Sie die IP-Version, für die Sie die DHCP-Option erstellen.

   Code: Wählen Sie den Code für die DHCP-Option, die Sie erstellen möchten.

   Hinweis – Mit dem Eintrag *filename* können Sie eine Datei angeben, die in den DHCP-Client geladen und dort ausgeführt werden soll. Mit *next-server* definieren Sie den

Boot-Server. Die nummerierten DHCP-Optionscodes werden unter anderem in RFC 2132 definiert.

Name: Geben Sie einen aussagekräftigen Namen für diese Option ein.

Art: Nur verfügbar, wenn Sie einen Code mit dem Kommentar *(unknown)* ausgewählt haben. Wählen Sie den Datentyp der Option aus. Sie können zwischen den Datentypen *IP-Adresse*, *Text* und *Hex* wählen. Geben Sie je nach ausgewähltem Datentyp die passenden Daten in das entsprechende Feld darunter ein:

> **Adresse:** Wählen Sie den Host oder die Netzwerkgruppe mit der/den IP-Adresse (n), die mit dieser DHCP-Option an den DHCP-Client übermittelt werden soll (en).Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.
>
> **Text:** Geben Sie den Text ein, der mit dieser DHCP-Option an den DHCP-Client übermittelt werden soll.
>
> **Hex:** Geben Sie den Hexadezimalwert ein, der mit dieser DHCP-Option an den DHCP-Client übermittelt werden soll. Bitte beachten Sie, dass Sie die Gruppen aus zwei Hexadezimalziffern jeweils durch einen Doppelpunkt trennen müssen, z. B. `00:04:76:16:EA:62`).

Bereich: Legen Sie fest, unter welchen Bedingungen die DHCP-Option gesendet werden soll.

- **Allgemein:** Die DHCP-Option wird von allen definierten DHCP-Servern an alle DHCP-Clients gesendet.
- **Server:** Wählen Sie im Feld *Server* die DHCP-Server aus, die die DHCP-Option senden sollen. In diesem Feld werden alle DHCP-Server angezeigt, die auf der Registerkarte *DHCP-Server* definiert sind.
- **Host:** Fügen Sie im Feld *Host* die Hosts hinzu bzw. wählen Sie sie aus, denen die DHCP-Option bereitgestellt werden soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.
- **MAC-Präfix:** Geben Sie ein MAC-Präfix ein. Die DHCP-Option wird allen DHCP-Clients mit passender MAC-Adresse bereitgestellt.

- **Anbieter-ID:** Geben Sie eine Anbieter-ID oder das Präfix einer Anbieter-ID ein. Die DHCP-Option wird allen DHCP-Clients, auf die diese Zeichenfolge zutrifft, bereitgestellt.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue DHCP-Option wird in der Liste *DHCP-Optionen* angezeigt und ist sofort aktiv.

Um eine DHCP-Option zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

7.3 NTP

Im Menü *Netzwerkdienste > NTP* wird der NTP-Server für die angeschlossenen Netzwerke konfiguriert. Das *Network Time Protocol* (NTP) ist ein Protokoll, das Uhren von Computer-Systemen über IP-Netzwerke synchronisiert. Anstatt nur die Zeit von Sophos UTM zu synchronisieren – diese Funktion wird auf der Registerkarte *Verwaltung > Systemeinstellungen > Zeit und Datum* eingestellt – können Sie bestimmten Netzwerken explizit erlauben, diesen Synchronisierungsdienst ebenfalls zu verwenden.

Um die Benutzung von NTP-Zeitsynchronisierung für bestimmte Netzwerke zu ermöglichen, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den NTP-Server.**
   Klicken Sie auf den Schieberegler.
2. **Wählen Sie *Zugelassene Netzwerke* aus.**
   Wählen Sie die Netzwerke aus, die Zugriff auf den NTP-Server haben sollen, oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.
3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

8 Network Protection

In diesem Kapitel wird beschrieben, wie Sie die grundlegenden Network-Protection-Funktionen von Sophos UTM konfigurieren. Die Seite *Network-Protection-Statistik* im WebAdmin zeigt einen Überblick über Ereignisse im Angriffschutzsystem sowie über verworfene Datenpakete für Quell- und Zielhosts.In jedem Abschnitt befindet sich ein Link auf die *Details*. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Berichte-Bereichs des WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Hinweis – Sie können eine *Netzwerk-/Hostausnahme* oder eine *Bedrohungsausnahme* direkt hinzufügen, indem Sie auf das **Plus**-Symbol in der Liste *Advanced Threat Protection: Neueste Ereignisse* klicken.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Firewall
- NAT (Netzwerkadressumsetzung)
- Advanced Threat Protection
- Intrusion Prevention
- Server-Lastverteilung
- VoIP (Voice over IP)
- Erweiterte Einstellungen

8.1 Firewall

Im Menü *Network Protection* > *Firewall* können Sie Firewallregeln für das Gateway definieren und verwalten. Allgemein gesagt ist die Firewall der zentrale Teil des Gateways und dient in einem Netzwerk dazu, Verbindungen zu verhindern, die von der Sicherheitsrichtlinie verboten sind. Die Standardrichtlinie von Sophos UTM besagt, dass der gesamte Netzwerkverkehr blockiert und protokolliert wird. Ausnahmen stellen automatisch generierte Regelwerke dar, die von anderen Softwarekomponenten des Gateways benötigt werden, um funktionieren zu können. Diese automatisch generierten Regeln werden jedoch auf der Registerkarte *Firewall* >

Regeln nicht angezeigt. Diese Sicherheitsrichtlinie erfordert, dass Sie explizite Regeln für Netzwerkverkehr anlegen, der das Gateway passieren darf.

8.1.1 Regeln

Auf der Registerkarte *Network Protection > Firewall > Regeln* wird das Firewallregelwerk verwaltet. Beim Öffnen der Registerkarte werden standardmäßig nur benutzerdefinierte Firewallregeln angezeigt. Mit Hilfe der Auswahlliste oberhalb der Liste können Sie stattdessen einstellen, dass nur automatische Firewallregeln oder beide Typen von Regeln angezeigt werden. Automatische Firewallregeln werden mit einer eigenen Hintergrundfarbe dargestellt. Automatische Firewallregeln werden von UTM auf der Basis von ausgewählten Auswahlkästchen *Automatische Firewallregeln* in einer Ihrer Konfigurationen generiert, z. B. beim Anlegen von IPsec- oder SSL-Verbindungen.

Neu definierte Firewallregeln sind direkt nach der Erstellung standardmäßig deaktiviert. Automatische Firewallregeln und aktive benutzerdefinierte Firewallregeln werden der Reihe nach angewendet, bis die erste Regel zutrifft. Automatische Firewallregeln stehen immer oben auf der Liste. Die Reihenfolge der Abarbeitung von benutzerdefinierten Firewallregeln richtet sich dabei nach der Positionsnummer, d. h., wenn Sie über die Positionsnummer die Reihenfolge der Regeln ändern, ändern Sie gleichzeitig die Reihenfolge der Abarbeitung.

Warnung – Sobald eine Firewallregel zutrifft, werden die nachfolgenden Regeln nicht mehr beachtet. Die Reihenfolge ist daher sehr wichtig. Setzen Sie nie eine Regel mit den Einträgen *Any (Quelle) – Any (Dienst) – Any (Ziel) – Zulassen (Aktion)* an den Beginn Ihres Regelwerks, da diese Regel alle Pakete in beide Richtungen durch das Gateway lassen würde, ohne nachfolgende Regeln zu beachten.

Um eine Firewallregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Regeln* auf *Neue Regel*.**
   Das Dialogfeld *Neue Regel anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Gruppe: Die Option *Gruppe* dient dazu, Regeln logisch zusammenzufassen. Mit der Auswahlliste über der Liste können Sie die Regeln nach ihrer Gruppe filtern. Die Zugehörigkeit zu einer Gruppe hat nur Auswirkungen auf die Darstellung, aber keinen Einfluss auf die Abarbeitung der Regeln. Um eine Gruppe anzulegen, wählen Sie den Eintrag << *Neue Gruppe* >> und geben Sie einen aussagekräftigen Namen in das Feld *Name* ein.

Position: Die Positionsnummer legt die Priorität der Regel fest. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Sobald eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen.

Quellen: Fügen Sie Quellnetzwerkdefinitionen hinzu bzw. wählen Sie sie aus, die angeben, von welchem Host/welchen Hosts oder Netzwerken die Pakete stammen.

Tipp – Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

Dienste: Fügen Sie Dienstdefinitionen zur Beschreibung der Protokolle und bei TCP oder UDP die Quell- und Zielports der Pakete hinzu bzw. wählen Sie sie aus.

Ziele: Fügen Sie die Netzwerkdefinition des Ziels hinzu, die Zielhost(s) oder Zielnetzwerk(e) der Pakete angibt, oder wählen Sie sie aus.

Hinweis – Wenn Sie mehr als eine Quelle, einen Dienst oder ein Ziel auswählen, gilt die Regel für alle möglichen Quelle-Dienst-Ziel-Kombinationen. Eine Regel mit zwei Quellen, zwei Diensten und zwei Zielen entspricht beispielsweise acht individuellen Regeln: von jeder Quelle an jedes Ziel über beide Dienste.

Aktion: Die Aktion, die angibt, wie mit Datenverkehr verfahren wird, auf den die Regel zutrifft. Die folgenden Aktionen können ausgewählt werden:

- **Zulassen:** Die Verbindung wird zugelassen und Datenverkehr wird weitergeleitet.
- **Verwerfen:** Alle Pakete, die diese Bedingung erfüllen, werden ohne Rückmeldung an den Absender verworfen.
- **Ablehnen:** Verbindungsanfragen, die diese Bedingung erfüllen, werden aktiv zurückgewiesen. Der Absender erhält eine entsprechende ICMP-Nachricht.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
Zeitraum: Standardmäßig ist keine Zeitraumdefinition ausgewählt. Das bedeutet, dass die Regel immer gültig ist. Wenn Sie eine Zeitraumdefinition auswählen, wird die Regel

nur innerhalb der Zeitspanne gültig, die durch diese Zeitraumdefinition festgelegt ist. Weitere Informationen finden Sie unter *Zeitraumdefinitionen*.

Verkehr protokoll.: Wenn Sie diese Option wählen, wird die Protokollierung aktiviert und Pakete, auf die Regeln zutreffen, werden ins Firewall-Protokoll aufgenommen.

Quell-MAC-Adressen: Wählen Sie eine MAC-Adressdefinition aus, die die MAC-Adressen enthält, von denen die Pakete stammen. Wenn die Option ausgewählt ist, entsprechen Pakete nur dann dieser Regel, wenn ihre Quell-MAC-Adresse in der Definition aufgelistet ist. Beachten Sie, dass Sie nicht gleichzeitig eine MAC-Adressdefinition und die Quelle *Any* verwenden können.MAC-Adressdefinitionen werden auf der Registerkarte *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *MAC-Adressdefinitionen* definiert.

4. **Klicken Sie auf *Speichern*.**
   Die neue Regel wird in der Liste *Regeln* angezeigt.

5. **Aktivieren Sie die Firewallregel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

   Die Regel ist jetzt aktiv (Schieberegler ist grün).

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Über diese Schaltfläche wird ein Pop-up-Fenster mit einem Echtzeit-Protokoll der gefilterten Pakete geöffnet. Das sich regelmäßig aktualisierende Fenster zeigt die aktuelle Netzwerkaktivität. Die Hintergrundfarbe gibt an, welche Aktion angewendet wurde:

- Rot: Das Paket wurde verworfen (drop).
- Gelb: Das Paket wurde abgelehnt (reject).
- Grün: Das Paket wurde zugelassen (allow).
- Grau: Die Aktion konnte nicht bestimmt werden.

Das Live-Protokoll enthält auch Informationen darüber, welche Firewallregel dafür gesorgt hat, dass ein Paket abgelehnt wurde.Solche Informationen sind wichtig für die Fehlersuche im Regelwerk.
Mit der Suchfunktion können Sie das Firewallprotokoll nach bestimmten Einträgen durchsuchen. Die Suchfunktion erlaubt es sogar, Ausdrücke auszuschließen, indem Sie ein Minus

vor den Ausdruck schreiben, z. B. `-WebAdmin`, wodurch alle Zeilen ausgeblendet werden, die diesen Ausdruck enthalten.

Bei Aktivierung der Funktion *Autoscroll* wird im Fenster automatisch nach unten gescrollt, sodass stets die aktuellsten Ergebnisse angezeigt werden.

Nachfolgend finden Sie einige grundlegende Hinweise zur Konfiguration der Firewall:

- **Verworfene Broadcasts:** Alle Broadcasts werden standardmäßig verworfen. Diese Aktion wird auch nicht protokolliert (weitere Informationen hierzu unter Erweitert). Dies ist für NetBIOS-Netzwerke (z. B. Microsoft-Windows-Betriebssysteme) mit vielen Computern hilfreich, da die Broadcasts das Firewallprotokoll schnell volllaufen lassen. Um eine Regel für das Verwerfen von Broadcasts manuell zu definieren, gruppieren Sie die Definitionen der Broadcast-Adressen aller angeschlossenen Netzwerke und fügen Sie eine „global_broadcast“-Definition `255.255.255.255/255.255.255.255` hinzu. Fügen Sie dann eine Regel hinzu, die sämtlichen Verkehr zu diesen Adressen verwirft, und platzieren Sie die Regel ganz oben in Ihrer Firewall-Konfiguration. In Netzwerken mit viel Broadcast hat das auch positive Auswirkungen auf die Systemleistung.
- **IDENT-Verkehr ablehnen:** Wenn Sie den IDENT-Reverse-Proxy nicht nutzen möchten, können Sie Datenpakete an den Port `113` (IDENT) des internen Netzwerks ablehnen. Dies kann bei Diensten, die IDENT verwenden (z. B. FTP, SMTP und IRC), längere Zeitüberschreitungen verhindern.

  Hinweis – Bei der Nutzung von Maskierung kommen die IDENT-Anfragen für die maskierten Netzwerke auf den Maskierungsschnittstellen an.

- NAT verändert die Adressen der Datenpakete und hat somit Auswirkungen auf die Firewall-Funktionalität.
  - DNAT wird *vor* der Firewall ausgeführt. Die Firewall bearbeitet daher die bereits umgeschriebenen Datenpakete. Das müssen Sie bedenken, wenn Sie Regeln für DNAT-bezogene Dienste anlegen.
  - SNAT und Maskierung werden *nach* der Firewall ausgeführt. Die Firewall bearbeitet daher noch die Datenpakete mit der originalen Quelladresse.

Mit den Funktionen im Kopfbereich der Tabelle können Firewallregeln nach bestimmten Kriterien gefiltert und so übersichtlich dargestellt werden. Wenn Sie Gruppen angelegt haben, können Sie eine Gruppe aus der Auswahlliste wählen und sehen so alle Regeln, die zu dieser Gruppe gehören. Mit dem Suchfeld können Sie nach Stichworten oder auch nur Wortteilen suchen, zu denen die Regeln angezeigt werden sollen. Die Suche umfasst Quelle, Ziel, Dienst, Gruppenname und Kommentar einer Regel.

8.1.2 Country-Blocking

Auf der Registerkarte *Network Protection > Firewall > Country-Blocking* können Sie Datenverkehr aus bestimmten Ländern oder Gegenden bzw. Datenverkehr, der für bestimmte Länder oder Gegenden bestimmt ist, blockieren. Sie können entweder einzelne Länder/Gegenden oder ganze Kontinente blockieren. Das Blockieren erfolgt auf Basis der GeoIP-Informationen in der IP-Adresse des Hosts.

Um Country-Blocking zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Country-Blocking.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Länder* kann nun bearbeitet werden.

2. **Wählen Sie die Gegenden, die blockiert werden sollen.**
   Legen Sie mit Hilfe der Auswahllisten vor den Namen der Länder bzw. Gegenden den Blockierstatus fest:

   - **Alle:** Der gesamte Verkehr von oder zu dieser Gegend wird blockiert.
   - **Von:** Verkehr aus dieser Gegend wird blockiert.
   - **Nach:** Verkehr in diese Gegend wird blockiert.
   - **Aus:** Verkehr aus und in diese Gegend ist erlaubt.

   Tipp – Sie können auf einfache Weise den gleichen Blockierstatus für alle Länder/Gegenden einer Region auswählen. Wählen Sie dafür in der Auswahlliste vor der entsprechenden Region den gewünschten Blockierstatus aus.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.Verkehr von diesen oder in diese Gegenden wird jetzt entsprechend Ihrer Einstellungen blockiert. Beachten Sie, dass Sie auf der Registerkarte *Country-Blocking-Ausnahmen* Ausnahmen für die blockierten Länder/Gegenden anlegen können.

Tipp – Jeder Abschnitt auf dieser Seite kann mit Hilfe des Reduzieren-Symbols rechts neben der Kopfzeile des Abschnitts auf- und zugeklappt werden.

8.1.3 Country-Blocking-Ausnahmen

Auf der Registerkarte *Network Protection > Firewall > Country-Blocking-Ausnahmen* können Sie Ausnahmen für Länder definieren, die auf der Registerkarte *Country-Blocking* blockiert werden. Ausnahmen können angelegt werden für Verkehr zwischen einem blockierten Land/einer blockierten Gegend und bestimmten Hosts oder Netzwerken, unter Berücksichtigung von Richtung und Dienst des Verkehrs.

Um eine Country-Blocking-Ausnahme anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahme anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Ausnahme ein.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

   Diese nicht blockieren:

   - **Region:** Mit dieser Auswahlliste können Sie die Auswahl der Länder, die im Feld *Länder* angezeigt wird, einschränken.
   - **Länder:** Aktivieren Sie das Auswahlkästchen vor den Gegenden oder Ländern, für die Sie eine Ausnahme anlegen wollen.Um alle Länder gleichzeitig auszuwählen, klicken Sie auf das Auswahlkästchen *Alle auswählen*.

   Für alle Anfragen: Wählen Sie die Bedingung, für die das Country-Blocking aufgehoben werden soll. Sie können zwischen ausgehendem und eingehendem Verkehr wählen, mit Bezug auf die darunter ausgewählten Hosts/Netzwerke.

   - **Hosts/Netzwerke:** Fügen Sie die Hosts/Netzwerke hinzu oder wählen Sie sie aus, die Verkehr in die gewählten Länder versenden oder aus diesen empfangen dürfen – abhängig von der Einstellung in der Auswahlliste darüber. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Für diese Dienste: Fügen Sie die Dienste hinzu, die zwischen den gewählten Hosts/Netzwerken und den gewählten Ländern/Orten erlaubt sein sollen.

3. **Klicken Sie auf *Speichern*.**
   Die neue Country-Blocking-Ausnahme wird in der Liste *Country-Blocking-Ausnahmen* angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

8.1.4 ICMP

Auf der Registerkarte *Network Protection* > *Firewall* > *ICMP* können Sie die Einstellungen für das *Internet Control Message Protocol* (ICMP) konfigurieren. ICMP dient dazu, verbindungsrelevante Statusinformationen zwischen Hosts auszutauschen. Darüber hinaus ist es wichtig, um die Erreichbarkeit des Netzwerks zu testen, und zur Fehlerbehebung bei Netzwerkproblemen.

Das Erlauben von allem ICMP-Verkehr auf dieser Registerkarte hebt eventuelle ICMP-Einstellungen in der Firewall auf. Wenn Sie ICMP-Verkehr nur für bestimmte Hosts oder Netzwerke erlauben wollen, sollten Sie besser die Registerkarte *Firewall* > *Regeln* verwenden.

Allgemeine ICMP-Einstellungen

Die folgenden allgemeinen ICMP-Optionen sind möglich:

- **ICMP auf Gateway zulassen:** Bei Auswahl dieser Option antwortet das Gateway auf alle ICMP-Pakete.

- **ICMP über Gateway zulassen:** Bei Auswahl dieser Option werden ICMP-Pakete über das Gateway weitergeleitet, wenn die Pakete aus einem internen Netzwerk stammen, also einem Netzwerk ohne Standard-Gateway.

- **ICMP-Umleitungen protokollieren:** Die ICMP-Umleitungen werden von Routern gegenseitig verschickt, um eine bessere Route zu einem Paketziel zu finden. Router ändern daraufhin ihre Routing-Tabellen und leiten das Paket auf der vermeintlich besseren Route zum gleichen Ziel weiter. Wenn Sie diese Option wählen, werden alle ICMP-Umleitungen im Firewallprotokoll protokolliert.

Hinweis– Wenn diese Option aktiviert ist, gelten die ICMP-Einstellungen für alle ICMP-Pakete, einschließlich Ping und Traceroute – wenn sie über ICMP gesendet werden –, auch wenn die zugehörigen Ping- und Traceroute-Einstellungen deaktiviert sind.

Ping-Einstellungen

Das Programm *Ping* ist ein Computer-Netzwerk-Tool, mit dem man testen kann, ob ein bestimmter Host über ein IP-Netzwerk erreichbar ist. Ping sendet ICMP-*Echo-Anfrage*-Pakete an den Zielhost und lauscht auf Antworten in Form von ICMP-*Echo-Antwort*-Paketen. Aus Zeitintervallen und Antworthäufigkeiten schätzt Ping die Dauer des Paketumlaufs und die Paketverlustrate zwischen den Hosts.

Die folgenden Ping-Optionen sind möglich:

- **Gateway ist Ping-sichtbar:** Das Gateway antwortet auf ICMP- *Echo-Antwort*-Pakete. Diese Funktion ist standardmäßig eingeschaltet.
- **Von Gateway pingen:** Der Ping-Befehl kann auf dem Gateway verwendet werden. Diese Funktion ist standardmäßig eingeschaltet.
- **Gateway leitet Pings weiter:** Das Gateway leitet ICMP-*Echo-Anfrage*- und *Echo-Antwort*-Pakete weiter, die aus einem internen Netzwerk stammen, also einem Netzwerk ohne Standard-Gateway.

Hinweis – Wenn die Funktion aktiviert ist, lassen die Ping-Einstellungen auch Traceroute-ICMP-Pakete zu, selbst wenn die betreffenden Traceroute-Einstellungen deaktiviert sind.

Traceroute-Einstellungen

Das Programm *Traceroute* ist ein Computer-Netzwerk-Tool zur Bestimmung der Route, die von Paketen in einem IP-Netzwerk genommen wird. Es listet die IP-Adressen der Router auf, über die das versendete Paket transportiert wurde. Sollte der Pfad der Datenpakete kurzfristig nicht bestimmbar sein, wird ein Stern (*) an Stelle der IP-Adresse angezeigt. Nach einer bestimmten Zahl an Fehlversuchen wird die Überprüfung abgebrochen. Der Abbruch einer Überprüfung kann viele Gründe haben, der wahrscheinlichste ist jedoch, dass eine Firewall im Netzwerkpfad Traceroute-Pakete blockiert.

Die folgenden Traceroute-Optionen sind möglich:

- **Gateway ist Traceroute-sichtbar:** Das Gateway antwortet auf Traceroute-Pakete.
- **Gateway leitet Traceroute weiter:** Das Gateway leitet Traceroute-Pakete weiter, die aus einem internen Netzwerk stammen, also einem Netzwerk ohne Standard-Gateway.

Hinweis – Darüber hinaus werden auch die UDP-Ports für UNIX-Traceroute-Anwendungen geöffnet.

Hinweis – Wenn die Funktion aktiviert ist, lassen die Traceroute-Einstellungen auch Ping-Pakete zu, selbst wenn die betreffenden Ping-Einstellungen deaktiviert sind.

8.1.5 Erweitert

Auf der Registerkarte *Network Protection* > *Firewall* > *Erweitert* können Sie erweiterte Einstellungen für die Firewall und die NAT-Regeln vornehmen.

Helfer für Verbindungsverfolgung

Sogenannte „Helfer für die Verbindungsverfolgung" aktivieren Protokolle, die mehrere Netzwerkverbindungen nutzen, um auf Firewall- oder NAT-Regeln zugreifen zu können. Alle Verbindungen, die per Firewall abgewickelt werden, werden durch das Kernelmodul *conntrack* mitverfolgt: ein Prozess, der besser als *connection tracking* (Verbindungsverfolgung) bekannt ist. Einige Protokolle, wie FTP und IRC, benötigen mehrere offene Ports und erfordern deshalb spezielle Helfer für die Verbindungsverfolgung, damit sie korrekt funktionieren. Diese Helfer sind spezielle Kernelmodule, die dabei helfen, zusätzliche Verbindungen zu identifizieren, indem sie diese als zur Eingangsverbindung zugehörig markieren. Das tun sie, indem sie die zugehörigen Adressen aus dem Datenstrom auslesen.

Damit z. B. eine FTP-Verbindung korrekt funktioniert, muss ein FTP-Conntrack-Helfer ausgewählt werden. Der Grund hierfür liegt in den Eigenheiten des FTP-Protokolls, welches zunächst eine einzelne Verbindung, die FTP-Kontrollverbindung, aufbaut. Sobald Befehle über diese Verbindung laufen, werden andere Ports geöffnet, um den Rest der Daten zu transportieren, die zu dem jeweiligen Befehl gehören (z. B. Downloads oder Uploads). Das Problem hierbei ist, dass das Gateway nichts von den Extraports weiß, weil sie dynamisch ausgehandelt wurden. Aus diesem Grund kann das Gateway auch nicht wissen, dass es dem Server erlauben soll, sich mit dem Client über diese spezifischen Ports (aktive FTP-Verbindungen) zu verbinden, oder dass es Clients aus dem Internet erlauben soll, sich mit dem FTP-Server zu verbinden (passive FTP-Verbindungen).

Hier wird der FTP-Conntrack-Helfer aktiv. Dieser spezielle Helfer wird zur Verbindungsverfolgung hinzugefügt und durchsucht dann die Kontrollverbindung (normalerweise auf Port 21) nach spezifischen Informationen. Wenn er auf korrekte Informationen stößt, fügt er diese spezifischen Informationen zu einer Liste erwarteter Verbindungen hinzu, sodass sie als zugehörig zur Kontrollverbindung gelten.Das wiederum ermöglicht es dem Gateway, sowohl die FTP-Eingangsverbindung als auch die zugehörigen Verbindungen richtig zu verfolgen.

Verbindungsverfolgungshelfer stehen für die folgenden Protokolle zur Verfügung:

- FTP
- IRC (für DCC)
- PPTP
- TFTP

Hinweis – Das Helfer-Modul PPTP wird benötigt, wenn Sie PPTP-VPN-Dienste auf dem Gateway anbieten wollen. PPTP-Verbindungen können sonst nicht aufgebaut werden. Der Grund hierfür ist, dass das Protokoll PPTP zuerst eine Verbindung auf TCP-Port 1723 aufbaut, bevor es zur Verbindung mit dem Protokoll *Generic Routing Encapsulation* (GRE) wechselt, das ein eigenständiges IP-Protokoll ist. Wenn das Helfer-Modul PPTP nicht geladen ist, werden alle GRE-Pakete vom Gateway blockiert. Falls Sie aber das Helfer-Modul PPTP nicht laden möchten, können Sie Firewallregeln manuell hinzufügen, sodass GRE-Pakete für ein- und ausgehenden Datenverkehr zulässig sind.

Protokollhandhabung

TCP-Fensterskalierung ermöglichen: Das TCP Receive Window (RWin) gibt vor (in Byte), welche Datenmenge ein System während einer Verbindung puffern kann. Der Absender kann nur diese Datenmenge versenden, danach muss er auf eine Bestätigung und eine Fensteraktualisierung des Empfängers warten. Für eine effizientere Nutzung von Netzwerken mit hoher Bandbreite kann eine größere Fenstergröße verwendet werden. Allerdings kontrolliert das TCP-Fenstergrößenfeld den Datenfluss und ist auf zwei Byte bzw. eine Fenstergröße von 65.535 Byte beschränkt. Da das Größenfeld nicht erweitert werden kann, wird ein Skalierungsfaktor verwendet. TCP window scaling (TCP-Fensterskalierung) ist eine Kerneloption des TCP/IP-Stacks und kann dazu verwendet werden, die maximale Fenstergröße von 65.535 Byte auf 1 Gigabyte zu erweitern. Die Fensterskalierung ist standardmäßig aktiviert. Da einige Netzwerkgeräte wie Router, Lastverteiler, Gateways usw. die Fensterskalierung immer noch nicht durchgehend unterstützen, kann es notwendig sein, sie auszuschalten.

Strikte TCP-Sitzungsverwaltung verwenden: Standardmäßig erkennt das System vorhandene TCP-Verbindungen, die aufgrund eines Neustarts in der Verbindungsverfolgungstabelle nicht verwaltet werden. Interaktive Sitzungen, wie z. B. SSH und Telnet, werden daher nicht unterbrochen, wenn eine Schnittstelle vorübergehend nicht erreichbar ist. Sobald diese Option aktiviert ist, wird immer ein neuer 3-Wege-Handshake notwendig sein, um solche Sitzungen zu reaktivieren. Darüber hinaus erlaubt diese Option nicht, dass die

TCP-Verbindungsmethoden gleichzeitig offen sind, oder dass TCP Handshakes unterbricht. Es wird empfohlen, diese Option ausgeschaltet zu lassen.

Paketlänge validieren: Wenn diese Option aktiviert ist, prüft die Firewall die Datenpakete auf die minimale Länge, wenn das Protokoll ICMP, TCP oder UDP verwendet wird. Wenn die Datenpakete kürzer als die Minimalwerte sind, werden sie blockiert und es wird ein Eintrag im Firewallprotokoll angelegt.

Täuschungsschutz: Die Option „Täuschungsschutz" ist standardmäßig deaktiviert. Sie können zwischen den folgenden Einstellungen wählen:

- **Normal:** Das Gateway verwirft und protokolliert alle Datenpakete, die als Absenderadresse entweder die gleiche Quell-IP-Adresse enthalten wie die Schnittstelle oder die auf einer Schnittstelle ankommen, die eine Quell-IP-Adresse eines Netzwerks besitzt, die einer anderen Schnittstelle im Netzwerk zugeordnet ist.
- **Strikt:** Mit dieser Einstellung werden darüber hinaus alle Datenpakete verworfen und protokolliert, die zwar die richtige Ziel-IP-Adresse für eine bestimmte Schnittstelle im Netzwerk enthalten, allerdings über eine Schnittstelle, der sie nicht zugeordnet sind, im Netzwerk eintreffen, also an einer Schnittstelle, für die sie nicht bestimmt sind. Beispielsweise werden Pakete verworfen, die von einem externen Netzwerk an eine IP-Adresse der internen Schnittstelle geschickt wurden, die aber nur dafür vorgesehen ist, Pakete aus dem internen Netzwerk entgegenzunehmen.

Protokollierungsoptionen

FTP-Datenverbindungen protokollieren: UTM protokolliert alle Datenverbindungen (FTP-Datei- und Verzeichnisauflistungen). Die Protokolleinträge werden mit dem Ausdruck „FTP data" versehen.

Eindeutige DNS-Anfragen protokollieren: UTM protokolliert alle ausgehenden Anfragen an DNS-Server sowie deren Ergebnis. Die Protokolleinträge werden mit dem Ausdruck „DNS request" versehen.

Verworfene Broadcasts protokollieren: Standardmäßig verwirft die Firewall alle Broadcasts, die darüber hinaus auch nicht protokolliert werden. Wenn Sie die Broadcasts jedoch im Firewall-Protokoll benötigen, z. B. für Prüfungszwecke, wählen Sie die Option aus.

8.2 NAT

Im Menü *Network Protection > NAT* werden die NAT-Regeln des Gateways definiert und verwaltet. *Network Address Translation* (NAT) ist ein Verfahren, mit dem die Quell- und/oder

Zieladressen von IP-Paketen umgeschrieben werden, wenn sie einen Router oder ein Gateway passieren. Die meisten Systeme benutzen NAT, damit mehrere Hosts in einem privaten Netzwerk den Internetzugang über eine einzige öffentliche IP-Adresse nutzen können. Wenn ein Client ein IP-Paket an den Router schickt, wandelt NAT die Absenderadresse in eine andere, öffentliche IP-Adresse um, bevor es das Paket ins Internet weiterleitet. Kommt eine Antwort auf dieses Paket zurück, wandelt NAT die öffentliche Adresse wieder in die ursprüngliche IP-Adresse um und leitet das Paket an den Client weiter. Abhängig von den vorhandenen Systemressourcen ist NAT in der Lage, beliebig große interne Netzwerke zu verwalten.

8.2.1 Maskierung (Masquerading)

Maskierung (engl. masquerading) ist eine Sonderform der *Quellnetzwerkadressumsetzung* (engl. Source Network Address Translation, SNAT), bei der viele private IP-Adressen (typischerweise Ihr LAN mit privatem Adressraum) auf eine einzige öffentliche IP-Adresse (typischerweise Ihre externe Schnittstelle zum Internet) umgeschrieben werden, d. h. Sie verbergen interne IP-Adressen und Netzwerkinformationen nach außen. SNAT ist allgemeiner, da es ermöglicht, mehrere Quelladressen mehreren Zieladressen zuzuordnen.

Hinweis – Die Quelladresse wird nur umgesetzt, wenn das Paket das Gateway über die angegebene Schnittstelle verlässt. Des Weiteren ist die Quelladresse immer die aktuelle IP-Adresse dieser Schnittstelle, d. h. diese Adresse kann dynamisch sein.

Um eine Maskierungsregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Maskierung* auf *Neue Maskierungsregel*.**
   Das Dialogfeld *Neue Maskierungsregel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Netzwerk: Wählen Sie das zu maskierende (interne) Netzwerk aus.

   Schnittstelle: Wählen Sie die (externe) Netzwerkkarte aus, die mit dem Internet verbunden ist.

   Benutze Adresse: Wenn der Schnittstelle, die Sie gewählt haben, mehr als eine IP-Adresse zugewiesen ist (siehe *Schnittstellen & Routing* > *Schnittstellen* > *Zusätzliche Adressen*), können Sie hier bestimmen, welche IP-Adresse für die Maskierung verwendet werden soll.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Maskierungsregel wird in der Liste *Maskierung* angezeigt.

4. **Aktivieren Sie die Maskierungsregel.**
   Klicken Sie auf den Schieberegler, um die Maskierungsregel zu aktivieren.

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schalt- flächen.

Hinweis – Damit von den Clients aus dem internen Netzwerk eine Verbindung zum Internet aufgebaut werden kann, müssen Sie für die Firewall entsprechende Regeln anlegen.

IPsec-Pakete sind von Maskierungsregeln niemals betroffen. Um die Quelladresse von IPsec-Paketen umzusetzen, legen Sie eine Regel für SNAT oder Volles NAT an.

8.2.2 NAT

DNAT (Destination Network Address Translation, Zielnetzwerkadressumsetzung) und SNAT (*Source Network Address Translation*, Quellnetzwerkadressumsetzung) sind zwei spezielle Fälle von NAT. Mit SNAT wird die IP-Adresse des Hosts umgeschrieben, der die Verbindung initiiert hat. Das Gegenstück hierzu ist DNAT, das die Zieladresse der Datenpakete umschreibt. DNAT ist besonders nützlich, wenn ein internes Netzwerk private IP-Adressen verwendet und der Administrator einige Dienste von außen zugänglich machen will.

Das lässt sich am besten anhand eines Beispiels verdeutlichen: Ein Webserver mit der IP-Adres- se `192.168.0.20`, Port `80`, der in einem privaten Netzwerk mit dem Adressraum `192.168.0.0/255.255.255.0` steht, soll für Clients aus dem Internet erreichbar sein. Da der Adressraum `192.168.` privat ist, können Internet-basierte Clients Pakete nicht direkt an den Webserver schicken. Sie können aber mit der externen (öffentlichen) Adresse der UTM kom- munizieren. DNAT kann in diesem Fall Pakete an Port `80` der Firewall annehmen und diese zum internen Webserver weiterleiten.

Hinweis – *PPTP-VPN-Zugang* ist nicht kompatibel mit DNAT.

Im Gegensatz zur Maskierung, bei der die Zuordnung zur Adresse der primären Netz- werkschnittstelle erfolgt, ordnet SNAT die Quelladresse der Adresse zu, die in der SNAT-Regel angegeben ist.

1:1-NAT ist ein Spezialfall von DNAT oder SNAT. In diesem Fall werden sämtliche Adressen eines Netzwerks 1:1 in die Adressen eines anderen Netzwerks mit der gleichen Netzmaske übersetzt. Die erste Adresse des ursprünglichen Netzwerks wird also in die erste Adresse des anderen Netzwerks übersetzt, die zweite in die zweite usw. Eine 1:1-NAT-Regel kann entweder auf die Quell- oder die Zieladresse angewendet werden.

> **Hinweis –** Der Port `443` (HTTPS) wird standardmäßig für das Benutzerportal genutzt.Wenn Sie den Port `443` an einen internen Server weiterleiten möchten, müssen Sie den Wert des TCP-Ports des Benutzerportals ändern (z. B. `1443`). Nehmen Sie diese Einstellung auf der Registerkarte *Verwaltung* > *Benutzerportal* > *Erweitert* vor.

Da DNAT vor dem Firewalling angewendet wird, müssen Sie sicherstellen, dass entsprechende Firewallregeln gesetzt sind. Weitergehende Informationen finden Sie unter *Network Protection* > *Firewall* > *Regeln*.

Um eine NAT-Regel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *NAT* auf *Neue NAT-Regel*.**
   Das Dialogfeld *Neue NAT-Regel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Gruppe: Die Option *Gruppe* dient dazu, Regeln logisch zusammenzufassen. Mit der Auswahlliste über der Liste können Sie die Regeln nach ihrer Gruppe filtern. Die Zugehörigkeit zu einer Gruppe hat nur Auswirkungen auf die Darstellung, aber keinen Einfluss auf die Abarbeitung der Regeln. Um eine Gruppe anzulegen, wählen Sie den Eintrag << *Neue Gruppe* >> und geben Sie einen aussagekräftigen Namen in das Feld *Name* ein.

   Position: Die Positionsnummer legt die Priorität der Regel fest. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Sobald eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen.

   Regeltyp: Wählen Sie den NAT-Modus aus. Abhängig vom gewählten Modus werden verschiedene Optionen angezeigt: Die folgenden Modi sind möglich:

   - **SNAT (Quelle):** Ordnet die Quelladresse definierter IP-Pakete einer neuen Quelladresse zu. Der Dienst kann ebenfalls geändert werden.

   - **DNAT (Ziel):** Ordnet die Zieladresse definierter IP-Pakete einer neuen Zieladresse zu. Der Dienst kann ebenfalls geändert werden.

- **1:1-NAT (gesamte Netzwerke):** Ordnet IP-Adressen eines Netzwerks 1:1 einem anderen Netzwerk zu. Die Regel gilt entweder für die Quell- oder die Zieladresse der definierten IP-Pakete.
- **Volles NAT (Quelle und Ziel):** Ordnet sowohl die Quell- als auch die Zieladresse definierter IP-Pakete einer neuen Quell- und einer neuen Zieladresse zu. Der Quelldienst und der Zieldienst können ebenfalls geändert werden.
- **Kein NAT:** Bei dieser Option handelt es sich um eine Ausnahmeregel. Beispiel: Wenn für ein bestimmtes Netzwerk eine NAT-Regel existiert, können Sie eine *Kein NAT*-Regel für bestimmte Hosts innerhalb dieses Netzwerks festlegen. Diese Hosts werden dann vom NAT ausgenommen.

Bedingung für Übereinstimmung: Wählen Sie Quell- und Zielnetzwerk, Quell- und Zielhost sowie den Dienst, für den Sie Adressen übersetzen möchten, oder fügen Sie diese Elemente hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

- **Datenverkehrsquelle:** Die ursprüngliche Quelladresse der Pakete. Dabei kann es sich entweder um einen einzelnen Host, ein gesamtes Netzwerk oder, außer für den Regeltyp *1:1-NAT*, einen Netzwerkbereich handeln.
- **Datenverkehrsdienst:** Der ursprüngliche Diensttyp des Pakets, der aus Quell- und Zielports der Pakete sowie einem Protokoll besteht.

  Hinweis – Ein Datenverkehrsdienst kann nur umgesetzt werden, wenn auch die entsprechenden Adressen umgesetzt werden. Des Weiteren kann ein Dienst nur in einen Dienst mit dem gleichen Protokoll umgesetzt werden.

- **Datenverkehrsziel:** Die ursprüngliche Zieladresse der Pakete. Dabei kann es sich entweder um einen einzelnen Host oder ein gesamtes Netzwerk handeln. Bei *SNAT* und *Kein NAT* kann es sich auch um einen Netzwerkbereich handeln.

Aktion: Wählen Sie den Quell- bzw. Ziel- bzw. Diensttyp, in den Sie die ursprünglichen IP-Paketdaten übersetzen möchten. Die angezeigten Parameter hängen vom ausgewählten *Regeltyp* ab. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

- **Quelle ändern in** (nur in den Modi *SNAT* oder *Volles NAT*): Wählen Sie den Quellhost, also die neue Quelladresse der Pakete.

- **Ziel ändern in** (nur in den Modi *DNAT* oder *Volles NAT*): Wählen Sie den Zielhost, also die neue Zieladresse der Pakete.
- **Dienst ändern in** (nur in den Modi *DNAT*, *SNAT* oder *Volles NAT*): Wählen Sie den neuen Dienst für die Pakete. Je nach ausgewähltem *Regeltyp* kann es sich hierbei um den Quell- bzw. Zieldienst handeln.
- **1:1-NAT-Modus** (nur im Modus *1:1-NAT*): Wählen Sie einen der folgenden Modi:
  - **Ziel zuordnen:** Ändert die Zieladresse.
  - **Quelle zuordnen:** Ändert die Quelladresse.

  Hinweis – Sie müssen im Feld *Datenverkehrsquelle* ein ganzes Netzwerk eingeben, wenn Sie die Quelle zuordnen möchten, oder im Feld *Datenverkehrsziel*, wenn Sie das Ziel zuordnen möchten.

- **Ziel** (nur im Modus *1:1-NAT*): Wählen Sie das Netzwerk, in das Sie die ursprüngliche IP-Adresse übersetzen möchten. Bitte beachten Sie, dass die Netzmaske des ursprünglichen Netzwerks mit der Netzmaske des übersetzten Netzwerks übereinstimmen muss.

Automatische Firewallregel (optional): Wählen Sie diese Option, um Firewallregeln automatisch zu generieren, sodass der entsprechende Datenverkehr die Firewall passieren kann.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Regel gilt für IPsec-Pakete (nur in den Modi *SNAT* oder *Volles NAT*): Wählen Sie diese Option, wenn die Regel für Datenverkehr gelten soll, der von IPsec verarbeitet wird. Diese Option ist standardmäßig nicht ausgewählt, wodurch IPsec-Verkehr von SNAT ausgeschlossen wird.

   Initpakete protokollieren (optional): Wählen Sie diese Option, um Initialisierungspakete einer Kommunikation ins Firewall-Protokoll zu schreiben. Wann immer eine NAT-Regel verwendet wird, werden Sie eine Meldung im Firewallprotokoll mit folgendem Inhalt finden: „Connection using NAT“ (dt. Verbindung benutzt NAT). Diese Option funktioniert sowohl für zustandbehaftete (stateful) als auch zustandlose (stateless) Protokolle.

4. **Klicken Sie auf *Speichern*.**
   Die neue Regel wird in der Liste *NAT* angezeigt.

5. **Aktivieren Sie die NAT-Regel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

8.3 Advanced Threat Protection

Im Menü *Network Protection > Advanced Threat Protection* können Sie die Funktion Advanced Threat Protection aktivieren und konfigurieren, damit infizierte oder gefährdete Clients innerhalb Ihres Netzwerks rasch erkannt werden und eine Warnung ausgegeben wird bzw. der entsprechende Verkehr verworfen wird. Advanced Threat Protection ist auf typische Herausforderungen in modernen Unternehmensnetzwerken ausgelegt: einerseits die Verwaltung mobiler Mitarbeiter mit immer mehr verschiedenen Mobilgeräten (BYOD), andererseits die immer schneller voranschreitende Weiterentwicklung und Verteilung von Schadsoftware. Advanced Threat Protection analysiert Netzwerkverkehr, z. B. DNS-Anfragen, HTTP-Anfragen oder IP-Pakete im Allgemeinen, die aus allen Netzwerken stammen bzw. an diese gesendet werden können. Advanced Threat Protection bietet zudem Angriffschutz und Antivirusdaten, wenn die entsprechenden Funktionen aktiviert sind. Die Datenbank zur Identifizierung von Bedrohungen wird laufend durch einen CnC/Botnet-Datenfeed von Sophos Labs mittels Pattern-Aktualisierungen aktualisiert.Anhand dieser Daten können infizierte Hosts und ihre Kommunikation mit Command-and-Control (CnC)-Servern schnell identifiziert werden und es kann entsprechend darauf reagiert werden.

8.3.1 Allgemein

Auf der Registerkarte *Advanced Threat Protection > Allgemein* können Sie das *Advanced Threat Protection System* der Sophos UTM aktivieren.

Um Advanced Threat Protection zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie das Advanced Threat Protection System.**
   Klicken Sie auf den Schieberegler.

Der Schieberegler wird gelb und der Bereich *Allgemeine Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Richtlinie: Wählen Sie die Sicherheitsrichtlinie aus, die vom Advanced Threat Protection System verwendet werden soll, wenn eine Bedrohung erkannt wurde.

   - **Verwerfen:** Das Datenpaket wird protokolliert und verworfen.
   - **Warnung:** Das Datenpaket wird protokolliert.

   Netzwerk-/Hostausnahmen: Fügen Sie die Quellnetzwerke oder -hosts hinzu, die vom Scannen auf Bedrohungen durch Advanced Threat Protection ausgenommen werden sollen, oder wählen Sie sie aus. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Bedrohungsausnahmen: Fügen Sie Ziel-IP-Adressen oder Domänennamen hinzu, die beim Scannen auf Bedrohungen durch Advanced Threat Protection übersprungen werden sollen. An dieser Stelle können Sie Falschmeldungen hinzufügen, um zu verhindern, dass sie als Bedrohung erkannt werden.Beispiele: `8.8.8.8` oder `google.com`.

   Achtung – Gehen Sie beim Festlegen von Ausnahmen mit Vorsicht vor. Wenn Sie Quellen oder Ziele ausnehmen, setzen Sie Ihr Netzwerk möglicherweise ernsthaften Gefahren aus.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Wenn diese Option aktiviert ist und eine Bedrohung erkannt wird, wird sie auf der Seite von Network Protection aufgelistet. Der Administrator erhält eine Benachrichtigung, wenn diese Funktion auf der Seite *Verwaltung > Benachrichtigungen > Benachrichtigungen* aktiviert ist. Die Benachrichtigung ist standardmäßig auf Verwerfen oder Warnung eingestellt.

Live-Protokoll

Das Live-Protokoll von Advanced Threat Protection kann zur Überwachung der erkannten Bedrohungen verwendet werden. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

Hinweis – IPS- und Web-Proxy-Bedrohungen werden im *Live-Protokoll* nicht angezeigt.

8.4 Intrusion Prevention

Im Menü *Network Protection > Intrusion Prevention* werden die IPS-Regeln des Gateways definiert und verwaltet. Das *Angriffsschutzsystem* (Intrusion Prevention System, IPS) erkennt Angriffsversuche anhand eines signaturbasierten IPS-Regelwerks. Das System analysiert den gesamten Datenverkehr und blockiert Attacken automatisch, bevor diese das lokale Netzwerk erreichen. Das bereits vorhandene Regelwerk und die Angriffsmuster werden durch die Pattern-Updates-Funktion aktualisiert. Neue IPS-Angriffs-Pattern-Signaturen werden automatisch als IPS-Regeln in das IPS-Regelwerk importiert.

8.4.1 Allgemein

Auf der Registerkarte *Network Protection > Intrusion Prevention > Allgemein* können Sie das *Angriffsschutzsystem* (Intrusion Prevention System, IPS) von Sophos UTM aktivieren.

Um IPS zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie das Angriffsschutzsystem.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Allgemeine IPS-Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Lokale Netzwerke: Fügen Sie Sie die Netzwerke hinzu oder wählen Sie die Netzwerke aus, die vom Angriffsschutzsystem überwacht werden sollen. Falls kein Netzwerk ausgewählt ist, wird IPS automatisch wieder ausgeschaltet und kein Netzwerkverkehr überwacht. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Richtlinie: Wählen Sie die Sicherheitsrichtlinie aus, die vom Angriffsschutzsystem verwendet werden soll, wenn eine IPS-Regel eine IPS-Angriffssignatur erkennt.

   - **Unbemerkt verwerfen:** Die Datenpakete werden ohne weitere Maßnahmen verworfen.

   - **Verbindung beenden:** An beide Verbindungspartner wird ein Paket geschickt, das die Verbindung beendet (*RST* bei TCP-Verbindungen und *ICMP Port Unreachable* für UDP-Verbindungen).

> **Hinweis –** Standardmäßig ist *Unbemerkt verwerfen* ausgewählt. Diese Einstellung sollte in der Regel nicht verändert werden, vor allem da aus Paketen zur Verbindungsbeendigung mutmaßliche Angreifer auch Informationen über das Gateway ziehen können.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Live-Protokoll

Das Intrusion-Prevention-Live-Protokoll dient zur Überwachung der gewählten IPS-Regeln.Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

8.4.2 Angriffsmuster

Die Registerkarte *Network Protection > Intrusion Prevention > Angriffsmuster* enthält das IPS-Regelwerk, gruppiert nach üblichen Angriffsmustern. Die IPS-Angriffsmuster sind in folgende Gruppen unterteilt:

- **Operating System Specific Attacks:** Angriffe auf Betriebssystem-spezifische Schwächen
- **Attacks Against Servers:** Angriffe auf alle Arten von Servern (z. B. Webserver, Mailserver)
- **Attacks Against Client Software:** Angriffe auf Client-Software (z. B. Webbrowser, Multimedia-Player)
- **Protocol Anomaly:** Die Angriffs-Patterns sind auf Netzwerkanomalien ausgerichtet.
- **Schadsoftware:** Software, die darauf ausgelegt ist, in ein Computersystem einzudringen und ihm zu schaden, ohne dass der Besitzer davon Kenntnis hat, z. B. Trojaner, DoS-Kommunikationswerkzeuge usw.

Um die Leistungsfähigkeit zu erhöhen, sollten Sie IPS-Angriffsmuster deaktivieren, die sich auf Dienste oder Software beziehen, welche nicht in Ihrem lokalen Netzwerk vorkommen. Wenn sich in Ihrem lokalen Netzwerk z. B. kein Webserver im Einsatz befindet, können Sie die Auswahl *HTTP-Server* aufheben.

Für jede Gruppe sind die folgenden Einstellungen verfügbar:

Aktion: Jede Regel einer Gruppe besitzt eine ihr zugewiesene Aktion. Sie können zwischen den folgenden Aktionen wählen:

- **Verwerfen:** Standardeinstellung. Wenn ein vermeintlicher Angriff festgestellt wird, werden die betroffenen Datenpakete verworfen.
- **Warnung:** Im Gegensatz zu *Verwerfen* wird das kritische Datenpaket durch das Gateway gelassen, aber es wird eine Warnmeldung in das IPS-Protokoll geschrieben.

Hinweis – Um die Einstellungen für individuell erstellte IPS-Regeln zu ändern, verwenden Sie auf der Registerkarte *Intrusion Prevention > Erweitert* das Feld *Geänderte Regeln*.Eine detaillierte Liste mit allen IPS-Regeln, die in Sophos UTM9 verwendet werden, finden Sie auf der UTM-Website.

Alter von Regeln: Standardmäßig sind IPS-Patterns auf diejenigen der letzten 12 Monate beschränkt. Sie können in Abhängigkeit von individuellen Faktoren wie dem Patch-Stand insgesamt, älteren Systemen oder anderen Sicherheitsanforderungen einen anderen Zeitraum wählen. Wenn Sie einen kürzeren Zeitraum wählen, reduziert sich die Anzahl an Regeln und die Leistung verbessert sich.

Extra-Warnungen hinzufügen: Wenn Sie diese Option wählen, werden jeder IPS-Regel zusätzliche Regeln hinzugefügt, die die IPS-Erkennungsrate erhöhen. Beachten Sie dabei, dass diese zusätzlichen Regeln allgemeiner gefasst und vager sind als die expliziten IPS-Angriffsmuster und dadurch sicherlich häufiger Alarme auslösen.Aus diesem Grund ist die voreingestellte Aktion für diese Regeln *Warnen*, welche nicht konfiguriert werden kann.

Benachrichtigen: Wenn Sie diese Option wählen, wird für jedes IPS-Ereignis, das zu dieser Gruppe gehört, eine Meldung an den Administrator geschickt. Beachten Sie, dass die Nachricht nur abgeschickt wird, wenn Sie die Benachrichtigungsfunktion auf der Registerkarte *Management > Benachrichtigungen > Benachrichtigungen* eingeschaltet und entsprechend konfiguriert haben. Darüber hinaus hängt es ebenfalls von den Einstellungen dort ab, ob es sich bei der Benachrichtigung um eine E-Mail oder SNMP-Trap handelt. Dabei kann es bis zu fünf Minuten dauern, bevor die Änderungen an den Benachrichtigungseinstellungen wirksam werden.

8.4.3 Anti-DoS/Flooding

Auf der Registerkarte *Anti-DoS/Flooding* können Sie die Konfiguration für den Schutz vor *Denial-of-Service*-Angriffen (DoS) und *Distributed-Denial-of-Service*-Angriffen (DDoS) vornehmen.

Allgemein gesagt, zielen DoS- und DDoS-Angriffe darauf ab, ein Computersystem für legitime Zugriffe unerreichbar zu machen. Im einfachsten Fall überflutet der Angreifer den Server mit sinnlosen Paketen, um diesen zu überlasten. Da für diese Angriffe eine große Bandbreite erforderlich ist, verlegen sich immer mehr Angreifer auf sogenannte *SYN-Flood-Attacken*, die nicht darauf abzielen, die Bandbreite auszulasten, sondern die Systemressourcen des Servers zu blockieren. Zu diesem Zweck werden sogenannte SYN-Pakete mit einer oftmals gefälschten Quelladresse an den TCP-Port des Dienstes geschickt. Auf diese Weise wird der Server veranlasst, die Verbindung zur Hälfte zu öffnen, indem er TCP/SYN-ACK-Pakete an die gefälschte Adresse zurücksendet und auf ein Antwort-TCP/ACK-Paket des Absenders wartet. Da die Absenderadresse gefälscht ist, wird dieses aber niemals kommen. Diese halboffenen Verbindungen sättigen die Anzahl der verfügbaren Verbindungen, die der Server eingehen kann, und hindern ihn daran, auf legitime Anfragen zu reagieren.

Solche Angriffe können abgewehrt werden, indem die Menge der SYN- (TCP), UDP- und ICMP-Pakete, die in das Netzwerk geschickt werden, über eine bestimmte Zeit begrenzt werden.

TCP-SYN-Flood-Schutz

Um den TCP-SYN-Flood-Schutz zu aktivieren, gehen Sie folgendermaßen vor:

1. **Wählen Sie auf der Registerkarte *Anti-DoS/Flooding* die Option *TCP-SYN-Flood-Schutz verwenden*.**

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Modus: Die folgenden Modi sind möglich:

   - **Quell- und Zieladressen:** In diesem Modus werden TCP-SYN-Pakete sowohl nach Quell-IP-Adresse als auch Ziel-IP-Adresse zurückgewiesen. Zunächst werden die SYN-Pakete, deren Quell-IP-Adresse übereinstimmt, auf die unten festgelegte Quellpaketrate begrenzt. Dann, wenn es immer noch zu viele Anfragen sind, werden diese zusätzlich anhand ihrer Ziel-IP-Adresse gefiltert und auf die Zielpaketrate begrenzt. Dieser Modus ist voreingestellt.

   - **Nur Zieladresse:** In diesem Modus werden die SYN-Pakete nur abhängig von der Ziel-IP-Adresse und der Zielpaketrate verworfen.

   - **Nur Quelladresse:** In diesem Modus werden die SYN-Pakete nur abhängig von der Quell-IP-Adresse und der Quellpaketrate verworfen.

   Protokollierung: Mit dieser Option können Sie den Protokollumfang einstellen. Die folgenden Protokollierungsstufen sind verfügbar:

- **Aus:** Wählen Sie diese Option, wenn keine Protokolle erstellt werden sollen.
- **Begrenzt:** Wählen Sie diese Option, um pro Sekunde maximal fünf Pakete zu protokollieren. Dieser Modus ist voreingestellt.
- **Alles:** Wählen Sie diese Option, um alle SYN-Verbindungsversuche (TCP) zu protokollieren. Beachten Sie, dass TCP-SYN-Flood-Angriffe schnell zu einer sehr umfangreichen Protokollierung führen können.

Quellpaketrate: Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Quell-IP-Adressen erlaubt sind.

Zielpaketrate: Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Ziel-IP-Adressen erlaubt sind.

Hinweis – Es ist wichtig, dass Sie in die Eingabefelder angemessene Werte eintragen. Wenn Sie die Werte zu hoch definieren, kann es passieren, dass der Webserver den Dienst versagt, weil er eine derart große Menge an TCP-SYN-Paketen nicht bewältigen kann. Wenn Sie andererseits die Rate zu gering definieren, kann es passieren, dass das Gateway unvorhersehbar reagiert und reguläre Anfragen blockiert. Es hängt hauptsächlich von Ihrer Hardware ab, welche Einstellungen für Sie sinnvoll sind. Ersetzen Sie daher die Standardeinstellungen durch für Ihr System geeignete Werte.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

UDP-Flood-Schutz

Der UDP-Flood-Schutz erkennt und blockiert UDP-Paketfluten.
Die Konfiguration des *UDP-Flood-Schutzes* ist identisch zu der des *TCP-SYN-Flood-Schutzes*.

ICMP-Flood-Schutz

Der ICMP-Flood-Schutz erkennt und blockiert ICMP-Paketfluten.
Die Konfiguration des *ICMP-Flood-Schutzes* ist identisch zu der des *TCP-SYN-Flood-Schutzes*.

8.4.4 Anti-Portscan

Auf der Registerkarte *Network Protection > Intrusion Prevention > Anti-Portscan* werden die Optionen für die Portscan-Erkennung konfiguriert.

Portscans werden meist von Hackern durchgeführt, um in gesicherten Netzwerken nach erreichbaren Diensten zu suchen: Um in ein System einzudringen bzw. eine DoS-Attacke zu starten, benötigen Angreifer Informationen zu den Netzwerkdiensten. Wenn solche Informationen vorliegen, sind Angreifer möglicherweise in der Lage, gezielt die Sicherheitslücken dieser Dienste auszunutzen. Netzwerkdienste, die die Internet-Protokolle TCP und UDP verwenden, sind über bestimmte Ports erreichbar und diese Port-Zuordnung ist im Allgemeinen bekannt, z. B. ist der Dienst SMTP in der Regel dem TCP-Port `25` zugeordnet. Die von Diensten verwendeten Ports werden als „offen“ bezeichnet, da es möglich ist, eine Verbindung zu ihnen aufzubauen, wohingegen unbenutzte Ports als „geschlossen“ bezeichnet werden, da Versuche, eine Verbindung zu ihnen aufzubauen, scheitern. Damit Angreifer herausfinden können, welche Ports offen sind, verwenden sie ein spezielles Software-Werkzeug, den Portscanner. Dieses Programm versucht mit mehreren Ports auf dem Zielhost eine Verbindung aufzubauen. Falls dies gelingt, zeigt es die entsprechenden Ports als offen an und die Angreifer haben die nötigen Informationen darüber, welche Netzwerkdienste auf dem Zielhost verfügbar sind.

Da den Internetprotokollen TCP und UDP je 65535 Ports zur Verfügung stehen, werden die Ports in sehr kurzen Zeitabständen gescannt. Wenn nun von derselben Quell-IP-Adresse mehrere Versuche registriert werden, mit immer anderen Ports Ihres Systems Verbindung aufzunehmen bzw. Informationen an diese zu senden, dann handelt es sich mit ziemlicher Sicherheit um einen Portscan. Wenn ein vermeintlicher Angreifer Hosts oder Dienste in Ihrem Netzwerk scannt, wird dies von der Portscan-Erkennung entdeckt. Eine Möglichkeit dagegen vorzugehen ist, weitere Portscans von derselben Quell-IP-Adresse automatisch zu blockieren. Beachten Sie, dass die Portscan-Erkennung auf Internetschnittstellen beschränkt ist, also Schnittstellen mit Standardgateway.

Technisch gesehen liegt ein Portscan vor, wenn für eine einzelne Quell-IP-Adresse innerhalb von 300 ms eine Erkennungsrate (engl. Detection Score) von 21 Punkten erreicht wird. Diese Erkennungsrate setzt sich folgendermaßen zusammen:

- Scan eines TCP-Zielports unter `1024` = 3 Punkte
- Scan eines TCP-Zielports gleich oder größer als `1024` = 1 Punkt

Um die Portscan-Erkennung zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Anti-Portscan* die *Portscan-Erkennung*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und der Bereich *Allgemeine Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Aktion: Die folgenden Aktionen sind möglich:

   - **Ereignis nur protokollieren:** Es wird keine Maßnahme gegen den Portscanner ergriffen. Das Ereignis wird nur protokolliert.
   - **Verkehr verwerfen:** Weitere Pakete des Portscans werden verworfen. Der Portscanner wird diese Ports als „gefiltert“ melden.
   - **Verkehr ablehnen:** Die Verbindungsanfragen des Angreifers werden zurückgewiesen und eine ICMP-Antwort „destination unreachable/port unreachable“ (Ziel/Port unerreichbar) wird an den Initiator geschickt. Der Portscanner wird diesen Port als „geschlossen“ melden.

   Protokollierung begrenzen: Aktivieren Sie diese Option, um die Menge der Protokollnachrichten zu begrenzen. Die Portscan-Erkennung kann während eines Portscans viele Einträge erzeugen. So wird z. B. jedes SYN-Paket, das als Teil eines Portscans angesehen wird, im Firewallprotokoll festgehalten. Durch Aktivierung dieser Funktion wird der Protokollumfang auf fünf Zeilen pro Sekunde reduziert.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

8.4.5 Ausnahmen

Auf der Registerkarte *Network Protection > Intrusion Prevention > Ausnahmen* können Sie Quell- und Zielnetzwerke definieren, die vom Angriffsschutzsystem (IPS) ausgenommen werden.

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahmenliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Ausnahme ein.

   Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, die nicht durchgeführt werden sollen:

   - **Angriffsschutz:** Wenn Sie diese Option aktivieren, wird das IPS von Sophos UTM ausgeschaltet.

- **Portscan-Schutz:** Wenn Sie diese Option aktivieren, verlieren Sie den Schutz vor Portscans, die Ihr System nach offenen Ports absuchen.
- **TCP-SYN-Flood-Schutz:** Wenn Sie diese Option aktivieren, wird der TCP-SYN-Flood-Schutz ausgeschaltet.
- **UDP-Flood-Schutz:** Wenn Sie diese Option aktivieren, wird der UDP-Flood-Schutz ausgeschaltet.
- **ICMP-Flood-Schutz:** Wenn Sie diese Option aktivieren, wird der ICMP-Flood-Schutz ausgeschaltet.

Für alle Anfragen: Wählen Sie mindestens eine Bedingung, für die die Sicherheitsprüfungen ausgesetzt werden sollen. Sie können mehrere Bedingungen logisch miteinander verknüpfen, indem Sie entweder *Und* oder *Oder* aus der Auswahlliste vor einer Bedingung auswählen. Die folgenden Bedingungen können konfiguriert werden:

- **Aus diesen Quellnetzwerken:** Wählen Sie diese Option, um Quellhosts/-netzwerke hinzuzufügen, die von Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Geben Sie die entsprechenden Hosts oder Netzwerke in das Feld *Netzwerke* ein, das nach Auswahl der Bedingung geöffnet wird.
- **Diese Dienste verwendend:** Wählen Sie diese Option, um Dienste hinzuzufügen, die von Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Fügen Sie die entsprechenden Dienste zum Feld *Dienste* hinzu, das nach Auswahl der Bedingung geöffnet wird.
- **Zu diesen Zielen gehend:** Wählen Sie diese Option, um Hosts/Netzwerke hinzuzufügen, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Geben Sie die entsprechenden Hosts oder Netzwerke in das Feld *Ziele* ein, das nach Auswahl der Bedingung geöffnet wird.

Tipp – Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

4. **Aktivieren Sie die Ausnahme.**
   Die neue Ausnahme ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler um die Ausnahme zu aktivieren.

   Die Ausnahme ist jetzt aktiv (Schieberegler ist grün).

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Hinweis – Wenn Sie Intrusion Prevention für Pakete mit der Zieladresse des Gateways ausschalten wollen, wird die Wahl *Any* im Feld *Ziele* nicht den gewünschten Effekt haben. Wählen Sie stattdessen eine Schnittstellendefinition des Gateways, die die IP-Adresse des Gateways enthält, z. B. *Internal (Address)*, wenn Sie Intrusion Prevention für die interne Adresse des Gateways ausschalten möchten.

8.4.6 Erweitert

Mustersatzoptimierung

Dateibezogene Muster aktivieren: Muster gegen dateibasierte Angriffe sind standardmäßig deaktiviert, da der Schutz vor solchen Bedrohungen üblicherweise von der Antivirus-Engine übernommen wird. Die Standardeinstellung (deaktiviert) maximiert die Leistung, bei aktivierter Option wird die Erkennungsrate maximiert. Die Aktivierung dateibezogener Muster kann sinnvoll sein, wenn kein anderer Virenschutz verfügbar ist, da z. B. Web Protection ausgeschaltet oder kein Client-Antiviren-Programm installiert ist.

Manuelle Regelmodifizierung

In diesem Bereich können Sie IPS-Regeln manuell modifizieren. Dabei wird die Standardrichtlinie, die aus den Gruppen unter Angriffsmuster stammt, für die jeweilige Regel überschrieben. Solche Änderungen sollten nur erfahrene Benutzer vornehmen.

Um eine modifizierte IPS-Regel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie im Feld *Geänderte Regeln* auf das Plussymbol.**
   Das Dialogfenster *Regel ändern* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Regel-ID: Tragen Sie die ID der IPS-Regel ein, die Sie ändern möchten. Die Regel-IDs finden Sie in der IPS-Regelliste auf der Sophos-Website. (In dem Ordner finden Sie

Dateien mit *IPS-rules* im Dateinamen, verfügbar für verschiedene UTM- und Musterversionen, sowohl im HTML- als auch im XML-Format). Darüber hinaus können sie auch über das IPS-Protokoll oder den IPS-Bericht bestimmt werden.

Diese Regel deaktivieren: Wenn Sie diese Option wählen, wird die IPS-Regel mit der entsprechenden ID ausgeschaltet.

Wenn Sie diese Option *nicht* auswählen, stehen die folgenden zwei Optionen zur Verfügung:

- **Benachrichtigungen ausschalten:** Wenn Sie diese Option wählen, werden keine Benachrichtigungen versendet, sofern diese Regel angewendet wurde.
- **Aktion:** Hierbei handelt es sich um die Aktionen, die ausgeführt werden, wenn eine Regel zutrifft. Sie können zwischen den folgenden Aktionen wählen:
    - **Verwerfen:** Wenn ein vermeintlicher Angriff festgestellt wird, werden die betroffenen Datenpakete verworfen.
    - **Warnung:** Im Gegensatz zu *Verwerfen* wird das kritische Datenpaket durch das Gateway gelassen, aber es wird eine Warnmeldung in das IPS-Protokoll geschrieben.

3. **Klicken Sie auf *Speichern*.**
   Die Regel wird im Feld *Geänderte Regeln* angezeigt. Bitte beachten Sie, dass Sie außerdem unten auf der Seite auf *Übernehmen* klicken müssen, damit die Änderungen wirksam werden.

Hinweis – Wenn Sie eine Regel-ID zum Feld *Geänderte Regeln* hinzufügen und die Aktion zum Beispiel auf *Warnung* setzen, wird die Änderung nur dann wirksam, wenn die Gruppe, zu der diese Regel gehört, auf der Registerkarte *Angriffsmuster* aktiv ist. Sollte diese Angriffsmustergruppe deaktiviert sein, haben Änderungen an einzelnen Regeln keine Auswirkung.

Leistungssteigerung

Um die Leistung des Angriffsschutzsystems zu verbessern und die Anzahl falscher Alarme zu minimieren, können Sie hier den Bereich der IPS-Regeln auf einzelne Ihrer internen Server begrenzen. Beispiel: Auf der Registerkarte *Angriffsmuster* ist die Gruppe *HTTP-Server* eingeschaltet und hier ist ein bestimmter HTTP-Server eingestellt. Wenn nun das Angriffsschutzsystem einen Angriff auf einen HTTP-Server feststellt, dann wird die eingestellte Aktion (*Verwerfen* oder *Warnung*) nur ausgeführt, wenn die IP-Adresse des betroffenen Servers mit der IP-Adresse des hier eingestellten HTTP-Servers übereinstimmt.

Der Einsatzbereich der IPS-Regeln kann für die folgenden Servertypen begrenzt werden:

- **HTTP:** Alle Untergruppen in der Angriffsmustergruppe *HTTP Servers*
- **DNS:** Die Angriffsmustergruppe *DNS*
- **SMTP:** Die Angriffsmustergruppen *Exchange* und *Sendmail*
- **SQL:** Alle Untergruppen in der Angriffsmustergruppe *Database Servers*

8.5 Server-Lastverteilung

Mit der Server-Lastverteilung-Funktion (server load balancing) können Sie eingehende Verbindungen (z. B. SMTP- oder HTTP-Verkehr) auf verschiedene Server hinter dem Gateway verteilen. Die Verteilung basiert auf der Quell-IP-Adresse mit einer Bindungsdauer von einer Stunde. Falls das Intervall zwischen zwei Anfragen derselben Quell-IP-Adresse diesen Zeitraum überschreitet, wird die Verteilung neu ausgehandelt. Die Verteilung des Datenverkehrs basiert auf einem einfachen Round-Robin-Algorithmus.

Alle Server des Serverpools werden entweder durch ICMP-Ping, TCP-Verbindungsaufbau oder HTTP/S-Anfragen überwacht. Bei einem Ausfall wird der betroffene Server nicht weiter verwendet, wobei jede eventuelle Quell-IP-Bindungsdauer aufgehoben wird.

Hinweis – Der Rückgabewert einer HTTP/S-Anfrage muss entweder `1xx Informational`, `2xx Success`, `3xx Redirection` oder `4xx Client Error` sein.Alle anderen Rückgabewerte werden als Fehler gewertet.

8.5.1 Verteilungsregeln

Auf der Registerkarte *Network Protection > Server-Lastverteilung > Verteilungsregeln* können Sie Lastverteilungsregeln für die Sophos UTM-Software festlegen. Nachdem Sie eine Regel erstellt haben, können Sie zusätzlich die Gewichtung der Lastverteilung zwischen den Servern und die Schnittstellenbindung festlegen.

Um eine Lastverteilungsregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verteilungsregeln* auf *Neue Lastverteilungsregel*.**
   Das Dialogfeld *Neue Lastverteilungsregel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Dienst: Wählen Sie den Netzwerkdienst aus, dessen Last Sie verteilen wollen.

Virtueller Server: Der ursprüngliche Zielhost des eingehenden Datenverkehrs. Üblicherweise entspricht die Adresse der externen Adresse des Gateways.

Echte Server: Die Hosts, die abwechselnd den Datenverkehr für diesen Dienst akzeptieren.

> **Tipp –** Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

Typ prüfen: Wählen Sie für die Dienstüberwachung entweder *TCP* (TCP-Verbindungsaufbau), *UDP* (UDP-Verbindungsaufbau), *Ping* (ICMP-Ping), *HTTP Host* (HTTP-Anfragen) oder *HTTPS Host* (HTTPS-Anfragen).Wenn Sie *UDP* verwenden, wird zunächst eine Ping-Anfrage versendet. Ist diese erfolgreich, folgt ein UDP-Paket mit der Payload 0. Ist der Ping erfolglos oder der ICMP-Port nicht erreichbar, gilt der Server als ausgefallen.Für *HTTP*- und *HTTPS*-Anfragen können Sie eine *URL* angeben, welche einen Hostnamen enthalten kann, aber nicht muss, z. B. `index.html` oder `http://www.beispiel.de/index.html`.

Intervall: Geben Sie einen Prüfintervall in Sekunden ein. Das Standardintervall beträgt 15 Sekunden, d. h. alle 15 Sekunden werden alle echten Server auf ihre Funktionsfähigkeit überprüft.

Zeitüberschreitung: Geben Sie eine maximale Zeitspanne in Sekunden ein, in der echte Server antworten müssen. Wenn ein Server in diesem Zeitraum nicht antwortet, gilt er als „tot".

Automatische Firewallregeln (optional): Wählen Sie diese Option, um automatisch Firewallregeln anlegen zu lassen. Diese Regeln erlauben die Weiterleitung von Datenverkehr von beliebigen Hosts zu den echten Servern.

Virtuelle Serveradresse abschalten (optional): Sie können diese Option nur aktivieren, wenn Sie eine zusätzliche Adresse als virtuellen Server für Lastverteilung verwenden (siehe Kapitel *Schnittstellen* > *Zusätzliche Adressen*). Sollten alle echten Server unerreichbar werden, schaltet sich diese zusätzliche Adressenschnittstelle automatisch ab.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Regel wird in der Liste *Verteilungsregeln* angezeigt.

4. **Aktivieren Sie die Lastverteilungsregel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

   Die Regel ist jetzt aktiv (Schieberegler ist grün).

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Beispiel: Angenommen, Sie besitzen in Ihrer DMZ zwei HTTP-Server mit den IP-Adressen `192.168.66.10` und `192.168.66.20`. Nun wollen Sie den HTTP-Verkehr, der auf der externen Schnittstelle des Gateways ankommt, gleichmäßig auf beide Server verteilen. Um eine Lastverteilungsregel zu erstellen, wählen Sie eine Hostdefinition oder legen Sie eine Hostdefinition für jeden Server an. Sie könnten sie *http_server_1* und *http_server_2* nennen. Wählen Sie dann im Dialogfeld *Neue Lastverteilungsregel erstellenHTTP* als *Dienst* aus. Wählen Sie außerdem die externe Adresse des Gateways als *Virtuellen Server* ausund fügen Sie zuletzt die Hostdefinitionen zum Feld *Echte Server* hinzu.

Gewichtung der Lastverteilung und Schnittstellenbindung

Zur Gewichtung der Lastverteilungs-Server und/oder zur Einstellung ihrer Schnittstellenbindung gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Bearbeiten* einer Lastverteilungsregel.**
   Das Dialogfeld *Lastverteilungsregel bearbeiten* wird geöffnet.
2. **Klicken Sie auf die Planer-Schaltfläche in der Kopfzeile des Feldes *Echte Server*.**
   Das Dialogfenster *Planer bearbeiten* wird geöffnet.
3. **Nehmen Sie die folgenden Einstellungen vor:**
   Gewichtung: Für die Gewichtung kann ein Wert zwischen 0 und 100 gewählt werden. Sie legen damit fest, wie viel Datenverkehr ein Server im Verhältnis zu allen anderen Servern verarbeitet. Hierfür wird ein gewichteter Round-Robin-Algorithmus verwendet, d. h. ein höherer Wert bedeutet, dass mehr Datenverkehr an den jeweiligen Server geroutet wird. Die Werte werden im Verhältnis zueinander bewertet, daher muss ihre Summe nicht 100 ergeben. Stattdessen können Sie zum Beispiel eine Konfiguration vornehmen, in der Server 1 den Wert 100, Server 2 den Wert 50 und Server 3 den Wert 0 hat. In diesem Fall verarbeitet Server 2 halb so viel Datenverkehr wie Server 1, während Server 3 nur beansprucht wird, wenn die anderen Server beide nicht verfügbar sind. Der

Wert 0 bedeutet in diesem Fall, dass, falls verfügbar, immer ein Server mit einem höheren Wert ausgewählt wird.

Bindung: Schnittstellenbindung (Interface Persistence) ist eine Methode, die sicherstellt, dass nachfolgende Verbindungen von einem Client immer über dieselbe Uplink-Schnittstelle geroutet werden. Die Bindung hat eine Zeitbeschränkung von einer Stunde. Sie können die Schnittstellenbindung für diese Lastverteilungsregel auch deaktivieren.

4. **Klicken Sie auf *Speichern*.**
   Das Dialogfenster *Planer bearbeiten* wird geschlossen und Ihre Einstellungen werden gespeichert.

5. **Klicken Sie auf *Speichern*.**
   Das Dialogfeld *Lastverteilungsregel bearbeiten* wird geschlossen.

8.6 VoIP

Voice over Internet Protocol (VoIP) ist der Sammelbegriff für das Routing von gesprochenen Konversationen über das Internet oder jedes andere IP-basierte Netzwerk. Sophos UTMunterstützt die am häufigsten eingesetzten Protokolle, um Sprachsignale über das IP-Netzwerk zu transportieren:

- SIP
- H.323

8.6.1 SIP

Das *Session Initiation Protocol* (SIP, dt. Sitzungsinitialisierungsprotokoll) ist ein Signalisierungsprotokoll zum Aufbau, zur Modifikation und zum Beenden von Sitzungen zwischen zwei oder mehreren Kommunikationspartnern. Das Protokoll wird hauptsächlich zum Aufbau und zum Beenden von Audio- oder Videotelefonieverbindungen eingesetzt. Um SIP zu nutzen, müssen Sie zuerst Ihre IP-Adresse und URLs bei Ihrem ISP registrieren. SIP nutzt UDP oder TCP auf Port `5060`, um auszuhandeln, welche IP-Adressen und Portnummern für den Austausch von Mediadaten (Video oder Sprache) zwischen den Endpoints verwendet werden sollen. Da durch das Öffnen des gesamten Port-Bereichs eine Sicherheitslücke entstehen würde, ist das Gateway in der Lage, den SIP-Datenverkehr „intelligent“ zu steuern. Dies wird durch einen speziellen Helfer für die Verbindungsverfolgung (engl. Connection Tracking Helper) erreicht, welcher durch Überwachung des Steuerkanals feststellt, welche dynamischen Ports

für die Verbindung genutzt werden, und daraufhin nur diese Ports für den Datenverkehr zulässt, wenn der Steuerkanal beschäftigt ist. Zu diesem Zweck müssen Sie sowohl einen SIP-Server als auch ein SIP-Clientnetzwerk angeben, um die entsprechenden Firewallregeln anzulegen, die die Kommunikation über das SIP-Protokoll ermöglichen.

Um die Unterstützung für das SIP-Protokoll zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die SIP-Protokoll-Unterstützung auf der Registerkarte *SIP*.** Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Allgemeine SIP-Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   SIP-Servernetzwerke: Hier können Sie die SIP-Server (die von Ihrem ISP bereitgestellt werden) hinzufügen oder auswählen, mit denen sich die SIP-Clients verbinden dürfen sollen. Wählen Sie aus Sicherheitsgründen nicht *Any* aus. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   SIP-Client-Netzwerke: Wählen Sie die Hosts oder Netzwerke der SIP-Clients aus, denen gestattet ist, eine SIP-Kommunikation zu beginnen oder anzunehmen, bzw. fügen Sie sie hinzu. Ein SIP-Client ist ein Endpunkt im LAN, der an einer Zweiwege-Kommunikation in Echtzeit mit einem anderen SIP-Client teilnimmt. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Erwartungsmodus: Wählen Sie aus, wie streng der Verbindungsaufbau gehandhabt werden soll:

   - **Strikt:** Eingehende Anrufe sind nur vom Registrar des ISPs erlaubt, d. h. von der IP-Adresse, an die die Nachricht REGISTER SIP gesendet wurde. Außerdem akzeptiert UTM nur Mediadatensitzungen (Sprache oder Video) von signalisierenden Endpoints, d. h. von den Geräten, die die SIP-Nachricht ausgetauscht haben. Manche Provider senden Mediadaten von einer anderen IP-Adresse als die SIP-Nachricht, was von UTM abgelehnt wird.

   - **Client-/Servernetzwerke:** Eingehende Anrufe sind von allen Clients der definierten SIP-Server- und SIP-Client-Netzwerke erlaubt. Mediadaten werden auch von einer anderen IP-Adresse akzeptiert als der, die die SIP-Nachricht geschickt hat, vorausgesetzt sie gehört zu einem der definierten SIP-Server- oder SIP-Cli-

ent-Netzwerke.

- **Any:** Sowohl eingehende Anrufe als auch Mediadaten sind von überall erlaubt.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

8.6.2 H.323

Das Protokoll H.323 ist ein internationaler Multimedia-Kommunikationsstandard, der von der *Internationalen Fernmeldeunion* (engl. International Telecommunication Union, ITU-T) veröffentlicht wurde. Es legt die Protokolle fest, mit denen audiovisuelle Kommunikationssitzungen auf jedem Netzwerk, das Pakete übermittelt, ermöglicht werden.H.323 wird üblicherweise für *Voice over IP* (VoIP) und IP-basierte Videokonferenzen genutzt.

H.323 nutzt standardmäßig TCP auf Port `1720`, um während des Telefonverbindungsaufbaus den dynamischen Port-Bereich zwischen den beiden Endpoints auszuhandeln. Da durch das Öffnen des gesamten Port-Bereichs eine Sicherheitslücke entstehen würde, ist das Gateway in der Lage, den H.323-Datenverkehr „intelligent" zu steuern. Dies wird durch einen speziellen Helfer für die Verbindungsverfolgung (engl. Connection Tracking Helper) erreicht, welcher durch Überwachung des Steuerkanals feststellt, welche dynamischen Ports für die Verbindung genutzt werden, und daraufhin nur diese Ports für den Datenverkehr zulässt, wenn der Steuerkanal beschäftigt ist. Zu diesem Zweck müssen Sie sowohl einen H.323-Gatekeeper als auch eine Client-Netzwerkdefinition angeben, um die entsprechenden Firewallregeln anzulegen, die die Kommunikation über das H.323-Protokoll ermöglichen.

Um die Unterstützung für das H.323-Protokoll zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die H.323-Protokoll-Unterstützung auf der Registerkarte *H.323*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Allgemeine H.323-Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   H.323-Gatekeeper: Wählen Sie einen H.323-Gatekeeper aus. Ein H.323-Gatekeeper kontrolliert alle H.323-Clients (Endpoints wie z. B. Microsoft NetMeeting) in seiner Zone. Genauer gesagt agiert er als Überwachungsinstanz aller H.323-Anrufe innerhalb seiner Zone im LAN. Seine wichtigste Aufgabe besteht darin, zwischen den symbolischen Alias-

Adressen und IP-Adressen zu übersetzen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

H.323-Client: Hier können Sie den Host oder das Netzwerk hinzufügen oder auswählen, zu dem und von dem aus H.323-Verbindungen aufgebaut werden. Ein H.323-Client ist ein Endpunkt im LAN, der an einer Zweiwege-Kommunikation in Echtzeit mit einem anderen H.323-Client teilnimmt. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Strikten Modus aktivieren (optional): Wählen Sie diesen Modus, um die Sicherheit zu verbessern. Falls Sie jedoch Verbindungsprobleme zu Ihrem ISP haben, deaktivieren Sie diese Option.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

8.7 Erweitert

Auf den Registerkarten im Menü *Network Protection > Erweitert* können Sie zusätzliche Funktionen für die Netzwerksicherheit konfigurieren: einen generischen Proxy, einen SOCKS-Proxy und einen IDENT-Reverse-Proxy.

8.7.1 Generischer Proxy

Der generische Proxy, auch bekannt als Port Forwarder, ist eine Kombination von DNAT und Maskierung (engl. masquerading) und leitet allen eingehenden Datenverkehr für einen bestimmten Dienst weiter zu einem beliebigen Server. Der Unterschied zum normalen DNAT ist jedoch, dass der generische Proxy auch die Quelladresse eines Anfragepakets mit der IP-Adresse der Schnittstelle für ausgehenden Datenverkehr ersetzt. Zusätzlich kann noch der Ziel-Port umgeschrieben werden.

Um eine Regel für den generischen Proxy anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Generischer Proxy* auf *Neue Generischer-Proxy-Regel*.**
   Das Dialogfeld *Neue Generischer-Proxy-Regel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Schnittstelle: Wählen Sie die Schnittstelle für den eingehenden Datenverkehr aus.

   Dienst: Fügen Sie die Dienstdefinition für den Verkehr hinzu, der weitergeleitet werden soll, oder wählen Sie sie aus.

   Host: Fügen Sie den Zielhost hinzu, zu dem der Datenverkehr weitergeleitet werden soll, oder wählen Sie ihn aus.

   Dienst: Fügen Sie den Zieldienst für den Verkehr hinzu, der weitergeleitet werden soll, oder wählen Sie ihn aus.

   Zugelassene Netzwerke: Fügen Sie die Netzwerke hinzu, zu denen die Weiterleitung erfolgen soll, oder wählen Sie sie aus.

   Tipp –Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Regel wird in der Liste *Generischer Proxy* angezeigt.

4. **Aktivieren Sie die Generischer-Proxy-Regel.**
   Die neue Regel ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Regel zu aktivieren.

   Die Regel ist jetzt aktiv (Schieberegler ist grün).

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

8.7.2 SOCKS-Proxy

SOCKS ist ein universelles Internet-Protokoll, durch das Client-Server-Anwendungen transparent die Dienste der Netzwerk-Firewall nutzen können. Der Proxy wird von vielen Client-Anwendungen hinter einer Firewall genutzt, um mit Hosts im Internet zu kommunizieren. Einige Beispiele dafür sind IRC-/Instant-Messaging-Clients, FTP-Clients und Windows SSH-/Telnet-Clients. Clients hinter einer Firewall, die auf einen externen Server zugreifen wollen, verbinden sich stattdessen mit einem SOCKS-Proxy-Server. Dieser Proxy-Server überprüft dann die Berechtigung des Clients, eine Verbindung zu dem externen Server aufzubauen, und leitet die

Anfrage zu dem Server weiter.Ihre Client-Anwendung muss explizit die Protokollversion SOCKS 4 oder SOCKS 5 unterstützen.

Der Standardport von SOCKS ist `1080`. Fast alle Clients verfügen über die Implementierung dieses Standardports, deshalb muss er normalerweise nicht konfiguriert werden. Die Unterschiede zwischen SOCKS und NAT sind, dass SOCKS auch „bind"-Anfragen erlaubt (im Auftrag des Clients auf einem Port lauschen – eine Funktion, die nur sehr wenige Clients unterstützen) und dass SOCKS 5 Benutzerauthentifizierung zulässt.

Wenn der SOCKS-Proxy eingeschaltet wird, muss mindestens ein Netzwerk ausgewählt werden, das Zugang zum Proxy hat. Für eine Benutzerauthentifizierung können auch die entsprechenden Benutzer oder Gruppen ausgewählt werden.

Hinweis – Ohne Benutzerauthentifizierung kann der SOCKS-Proxy sowohl mit dem SOCKS-4- als auch mit dem SOCKS-5-Protokoll genutzt werden. Für Benutzerauthentifizierung wird das Protokoll SOCKS 5 benötigt. Damit der Proxy im SOCKS-5-Modus Hostnamen auflöst, müssen Sie auch den DNS-Proxy einschalten. Andernfalls schlägt die DNS-Auflösung fehl.

Um den SOCKS-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den SOCKS-Proxy auf der Registerkarte *SOCKS-Proxy*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *SOCKS-Proxy-Optionen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Zugelassene Netzwerke: Fügen Sie die Netzwerke hinzu, die den SOCKS-Proxy verwenden dürfen, oder wählen Sie sie aus. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   Benutzerauthentifizierung aktivieren: Wenn Sie diese Option wählen, müssen Benutzer einen Benutzernamen und ein Kennwort angeben, um sich am SOCKS-Proxy anmelden zu können. Da Benutzerauthentifizierung nur vom Protokoll SOCKS 5 unterstützt wird, wird SOCKS 4 automatisch ausgeschaltet.

   Zugelassene Benutzer: Wählen Sie die Benutzer oder Gruppen aus, die Zugriff auf den SOCKS-Proxy haben sollen, oder fügen Sie die neuen Benutzer hinzu. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer* erläutert.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

8.7.3 IDENT-Reverse-Proxy

Das IDENT-Protokoll wird von einigen Remote-Servern zur einfachen Identitätsprüfung der auf sie zugreifenden Clients verwendet. Obwohl dieses IDENT-Protokoll unverschlüsselt ist und leicht manipuliert werden kann, verwenden es noch viele Dienste und setzen es manchmal sogar voraus.

Um den IDENT-Reverse-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die IDENT-Weiterleitung auf der Registerkarte *IDENT-Reverse-Proxy*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und der Bereich *Allgemeine Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   An interne Hosts weiterleiten (optional): Da IDENT-Anfragen von der Verbindungsverfolgung des Gateways nicht verarbeitet werden, bleiben sie „stecken", wenn Maskierung (engl. masquerading) verwendet wird. Wählen Sie die Option *An interne Hosts weiterleiten* aus, um IDENT-Anfragen an maskierte Hosts hinter dem Gateway weiterzuleiten. Beachten Sie dabei, dass die aktuelle IP-Verbindung nicht übergeben wird. Stattdessen wird das Gateway beim internen Client nach einer IDENT-Antwort fragen und diese Zeichenfolge an den anfragenden Server weiterleiten. Dieses Vorgehen wird von den meisten „Mini-IDENT"-Servern unterstützt, die meist Bestandteil der heute gängigen IRC- und FTP-Clients sind.

   Standardantwort: Das Gateway bietet Unterstützung für die Beantwortung von IDENT-Anfragen, wenn Sie die IDENT-Weiterleitung aktivieren. Das System wird dann immer mit der Zeichenfolge antworten, die Sie im Feld *Standardantwort* eingegeben haben, ungeachtet des lokalen Dienstes, der die Verbindung initiiert hat.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

9 Web Protection

In diesem Kapitel wird beschrieben, wie Sie die grundlegenden Web-Protection-Funktionen von Sophos UTM konfigurieren.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Webfilter
- Webfilter-Profile
- Filteroptionen
- Richtlinientest
- Application Control
- FTP

Die Seite *Web-Protection-Statistik* im WebAdmin enthält eine Übersicht mit den am meisten genutzten Anwendungen und Anwendungskategorien, den meistaufgerufenen Domänen hinsichtlich Zeit und Verkehr sowie den Top-Internet-Nutzern. Des Weiteren werden die meistblockierten Kategorien für die Websites angezeigt. In jedem Abschnitt befindet sich ein Link auf die *Details*. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Berichte-Bereichs des WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Hinweis – Detaillierte Informationen über die Erfassung der Internetnutzungsdaten und die Berechnung der Statistiken finden Sie auf der Seite *Protokolle & Berichte* > *Web Protection* > *Internetnutzung*.

Wenn Sie im Bereich *Häufigste Anwendungen* mit dem Mauszeiger über eine Anwendung fahren, werden ein oder zwei Symbole mit zusätzlichen Funktionen angezeigt:

- Klicken Sie auf das Symbol *Blockieren*, um die Anwendung ab diesem Moment zu blockieren. Auf der Seite *Application-Control-Regeln* wird dann eine Regel erstellt. Diese Option ist nicht für Anwendungen verfügbar, die für einen reibungslosen Betrieb von Sophos UTM relevant sind. So kann beispielsweise WebAdmin-Datenverkehr nicht blockiert werden, da dies dazu führen könnte, dass Sie nicht mehr auf den WebAdmin zugreifen können. Auch nicht klassifizierter Datenverkehr kann nicht blockiert werden.
- Klicken Sie auf das Symbol *Regeln*, um Traffic Shaping für die entsprechende Anwendung zu aktivieren. Ein Dialogfenster wird geöffnet, in dem Sie die Regeleinstellungen

vornehmen können. Klicken Sie auf *Speichern*, wenn Sie fertig sind. Dies erstellt jeweils eine Regel auf den Seiten Verkehrskennzeichner und Bandbreiten-Pools.
Traffic-Shaping ist nicht verfügbar, wenn Sie eine Flow-Monitor-Ansicht mit *allen Schnittstellen* ausgewählt haben, da Traffic-Shaping schnittstellenbasiert funktioniert.

9.1 Webfilter

Mit den Registerkarten des Menüs *Web Protection > Webfilter* können Sie Sophos UTM-Software als HTTP/S-Caching-Proxy konfigurieren. Der HTTP/S-Proxy von Sophos UTM bietet neben dem reinen Zwischenspeichern (Caching) zahlreiche Webfilterfunktionen für Netzwerke, die diesen Dienst verwenden dürfen. Das beinhaltet das Verhindern von Virus- und Spyware-Infektionen mit Hilfe von zwei unterschiedlichen Virenerkennungsmechanismen, deren Signaturdatenbanken laufend aktualisiert werden, und Spyware-Filtermechanismen, die sowohl eingehenden als auch ausgehenden Datenverkehr schützen. Außerdem kann Sophos UTM den Zugriff auf verschiedene Websites kontrollieren, indem es auf eine ausgeklügelte Website-Kategorisierung zurückgreift und dabei die weltweit größte Echtzeit-URL-Datenbank nutzt.In Verbindung mit der Sophos-Endpoint-Software kann Sophos UTM dieselben Web-Richtlinien auf Endpoint-Geräten in externen Netzwerken erzwingen und überwachen. Wie Sie *Endpoint Web Control* aktivieren, erfahren Sie unter *Endpoint Protection > Web Control*.

Sie können Ihre Filteraktionen auch auf der Registerkarte *Webfilter-Profil > Filteraktionen* verwalten. Dort können Sie Filteraktionen hinzufügen, bearbeiten, klonen oder löschen. Jetzt aber können Sie zudem den Assistenten *Filteraktion hinzufügen/bearbeiten* auf der Registerkarte *Webfilter > Richtlinien* zum Erstellen, Bearbeiten und Zuweisen von Filteraktionen verwenden.

9.1.1 Webfilter-Änderungen

Ab Version 9.2 umfasst Sophos UTM eine neue, vereinfachte Benutzeroberfläche zum Erstellen und Verwalten von Webfilterrichtlinien. Die Benutzeroberfläche hat sich zwar sehr geändert, die Funktionalität blieb jedoch unverändert. Alle Ihrer vorhandenen Einstellungen wurden beibehalten und wenn Sie keine Änderungen vornehmen, verhält sich das System genau gleich.

Bisher mussten für komplexe Webrichtlinien Webfilter-Profile angelegt werden. Diese bestanden aus Filteraktionen, die auf der Registerkarte *Filteraktionen* angelegt wurden und dann über Filterzuweisungen auf der Registerkarte *Filterzuweisungen* Benutzern und Gruppen zugewiesen wurden. Auf der Registerkarte *Proxy-Profile* wurden sie konfiguriert. Ab sofort kön-

nen Sie alle Aspekte Ihrer Webfilter-Richtlinien, einschließlich der Standardkonfiguration und erweiterter Filterprofile, auf der Registerkarte *Webfilter* > *Richtlinien* konfigurieren.

Hinweis –Nehmen Sie sich Zeit, um sich mit der neuen Benutzeroberfläche vertraut zu machen, und lesen Sie die folgende Übersicht. Auch wenn sich die aktuelle Version damit von älteren Versionen unterscheidet, sollte die Erstellung und Verwaltung komplexer Webrichtlinien nun sehr viel einfacher sein.

9.1.1.1 Wichtige Unterschiede

- Viele Registerkarten, die früher unter *Web Protection* > *Webfilter* zu finden waren, sind jetzt unter *Web Protection* > *Filteroptionen* verfügbar.
- Die neue UTM-Benutzeroberfläche beschreibt Webfilter-Regeln mittels Richtlinien. Eine Richtlinie ist das, was in vorherigen Versionen eine zugewiesene Filteraktion war.
- In Version 9.1 und älteren Versionen hatte das Standardprofil nur eine einzige Filterzuweisung (die Standardzuweisung genannt wurde). Ab Version 9.2 kann das Standardprofil mehrere Richtlinien umfassen.
- Die Ersatzaktion aus früheren Versionen wird jetzt als *Basisrichtlinie* bezeichnet. Ihre Funktion bleibt unverändert. Die Basisrichtlinie enthält die Filteraktion, die verwendet wird, wenn keine anderen Richtlinien zutreffen.
- Das Anlegen von Filteraktionen erfolgt nun über ein Dialogfeld mit mehreren Registerkarten – den *Filteraktionsassistenten*.
- Proxy-Profile heißen jetzt Filterprofile und können über die Registerkarte *Webfilter-Profile* > *Filterprofile* verwaltet werden.Die einem Filterprofil zugeordneten Richtlinien werden auf der Registerkarte *Richtlinien* in den Dialogfeldern *Profil bearbeiten* und *Profil hinzufügen* angezeigt.
- In 9.1 und früheren Versionen konnte eine einzelne Filterzuweisung in mehreren Proxy-Profilen verwendet werden. Ab Version 9.2 gehört eine Richtlinie zu einem einzigen Filterprofil.

9.1.1.2 Häufige Aufgaben

Es folgt ein kurzer Überblick über häufige Aufgaben und ihre Durchführung in 9.2 und späteren Versionen im Vergleich zur Benutzeroberfläche von Version 9.1.

Wie ...	**9.1**	**9.2**
... bearbeite ich die Standardrichtlinie?	Konfigurieren Sie die verschiedenen Registerkarten unter *Webfilter*: • *Webfilter > Antivirus/Schadsoftware* • *Webfilter > URL-Filterung* • *Webfilter > Erweitert*	*Webfilter > Richtlinien*
... erstelle oder bearbeite ich ein Proxy-Profil?	*Webfilter-Profile > Proxy-Profile*	Webfilter > Webfilter-Profile
... füge ich eine Ausnahme zu meiner Standardrichtlinie hinzu oder bearbeiten diese?	*Webfilter > Ausnahmen*	1. *Webfilter > Richtlinien* 2. Wählen Sie die *Standard-Filteraktion* für die *Basisrichtlinie aus* 3. Klicken Sie unter *Websitefilter* auf das grüne Plussymbol neben *Diese Websites blockieren/zulassen*
... weise ich einem Proxy-Profil eine Filterzuweisung zu?	1. Legen Sie unter *Webfilter-Profile > Filteraktionen eine Filteraktion an* 2. Erstellen Sie unter *Webfilter-Profile > Filterzuweisungen eine Filterzuweisung* 3. Bearbeiten oder ergänzen Sie unter *Webfilter-Profile > Proxy-Profile ein Proxy-Profil*	*Webfilter > Richtlinien*

9.1.1.3 Migration

Bei der Aktualisierung auf Version 9.2 bleiben Ihre bestehenden Konfigurationen und Einstellungen erhalten. Da sich jedoch die Benutzeroberfläche deutlich verändert hat, befinden sich einige Funktionen nicht mehr am gewohnten Ort. Es folgen ein paar Hinweise in Bezug auf Ihre Konfiguration.

Proxy-Profile heißen jetzt Filterprofile. Eines der ersten Dinge, das Ihnen auffallen wird, ist, dass nun jedes Filterprofil, einschließlich der Standardrichtlinie unter *Webfilter > Richtlinien*, über mehrere deaktivierte Richtlinien und eine oder mehrere aktivierte Richtlinien verfügt. Dies mag zunächst verwirrend erscheinen. Die Funktionalität entspricht jedoch der von Version 9.1. Durch die Änderungen ist es nun einfacher, Ihre Konfiguration zu aktualisieren, und Sie können die neuen Funktionen von 9.2 nutzen.

Nach der Aktualisierung enthalten Ihre Standardrichtlinie unter *Webfilter > Richtlinien* und Ihre Filterprofile unter *Webfilter-Profile > Filterprofile* möglicherweise eine Liste mehrerer deaktivierter Richtlinien.Beim Bearbeiten eines Profils in Version 9.1 wurde eine Liste von *Filterzuweisungen* mit Kontrollkästchen angezeigt, die entweder aktiviert oder deaktiviert waren. In 9.2 gibt es eine Liste von *Richtlinien*, die entweder aktiviert oder deaktiviert sind. Wenn Sie deaktivierte, migrierte Richtlinien sehen, so sind dies deaktivierte Filterzuweisungen aus Version 9.1.

Da Richtlinien zu einem einzigen Filterprofil gehören, legt die Migration in jedem Proxy-Profil eine Kopie jeder Filterzuweisung an. Das heißt, dass Sie eine Richtlinie in einem Profil löschen können, ohne dass dies Auswirkungen auf andere hat. Da für die meisten Profile die migrierten, deaktivierten Richtlinien nicht erforderlich sind, können Sie sie problemlos löschen.

Das Gleiche gilt für das Standardfilterprofil, das auf der Registerkarte *Webfilter > Richtlinien* angezeigt wird. In 9.1 wird die Standardfilterzuweisung in der UI nicht angezeigt; sie ist jedoch vorhanden. In 9.2 ist sie zu einer Richtlinie namens „xxxx“ migriert. Da das Standard-Proxy-Profil jetzt mehrere Richtlinien aufweisen kann, wurden die anderen Filterzuweisungen als deaktivierte Richtlinien migriert. Auch diese können gelöscht werden, wenn sie nicht benötigt werden.

Warum haben wir sie migriert, wenn wir Ihnen nun sagen, dass sie gelöscht werden können? Der Grund ist, dass Sie möglicherweise Ihre Einstellungen konsolidieren oder verschieben möchten. Beispielsweise könnten Sie in 9.1 ein zusätzliches Proxy-Profil erstellt haben, um so über mehrere Zuweisungen zu verfügen (dies war im Standardprofil von 9.1 nicht möglich). In 9.2 wurde diese Beschränkung aufgehoben und es ist einfacher, alles im Standardprofil

unterzubringen. Die Migration erfolgte, sodass Sie lediglich die Netzwerke Ihres Profils richtig einstellen und die migrierten Richtlinien aktivieren müssen. Dann können Sie die zusätzlichen Filterprofile löschen, um Ihre Konfiguration zu vereinfachen.

9.1.2 Allgemein

Auf der Registerkarte *Web Protection > Webfilter > Allgemein* können Sie die Grundeinstellungen für den Webfilter vornehmen.

Um den Webfilter zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den Webfilter auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und der Bereich *Primäres Webfilterprofil* kann nun bearbeitet werden.

2. **Wählen Sie die zugelassenen Netzwerke aus.**
   Wählen Sie die Netzwerke aus, die den Webfilter verwenden dürfen. Der Webfilter wartet standardmäßig auf Anfragen an TCP-Port `8080` und lässt jeden Client zu, der sich in einem Netzwerk befindet, das im Feld *Zugelassene Netzwerke* aufgeführt ist.

   > **Warnung –** Wählen Sie niemals das Netzwerkobjekt *Any* aus, weil Sie dadurch Ihre Appliance einem hohen Risiko für Angriffe aus dem Internet aussetzen würden.

3. **Wählen Sie die Optionen „HTTPS-Verkehr (SSL) scannen“ aus.**
   Wählen Sie eine Option zum Scannen des HTTPS-Verkehrs (SSL):
   - *Nicht scannen*: HTTPS-Verkehr wird nicht gescannt
   - *Nur URL-Filterung*: Prüfungen werden basierend auf der URL durchgeführt, der tatsächliche HTTPS-Datenverkehr wird jedoch nicht gescannt.
   - *Entschlüsseln und scannen*: Der Inhalt des HTTPS-Verkehrs wird vollständig entschlüsselt und gescannt.

4. **Wählen Sie einen Betriebsmodus aus.**
   Falls Sie einen Betriebsmodus mit Benutzerauthentifizierung wählen, sollten Sie auch die Benutzer und Gruppen angeben, die auf den Webfilter zugreifen dürfen. Die folgenden Betriebsmodi sind möglich:

   - **Standardmodus:** Im Standardmodus lauscht der Webfilter standardmäßig nach Client-Anfragen auf Port 8080 und lässt jeden Client zu, der sich in einem

Netzwerk befindet, das im Feld *Zugelassene Netzwerke* aufgeführt ist. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

Wählen Sie eine Authentifizierungsmethode aus:

- **Keine:** Wählen Sie diese Option, wenn keine Authentifizierung verwendet werden soll.
- **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

  Hinweis – Wenn Sie eine Active-Directory-Benutzergruppe anlegen, empfehlen wir dringend, im Feld *Active-Directory-Gruppen* die Namen der Active-Directory-Gruppen oder Benutzer direkt manuell einzugeben, statt die LDAP-Strings zu verwenden. Beispiel: Statt eines LDAP-Strings `CN=ads_group1,CN=Users,DC=example,DC=com` geben Sie einfach den Namen `ads_group1` ein.

  Hinweis – Wenn Sie Kerberos verwenden, geben Sie in das Feld *Active-Directory-Gruppen* nur Gruppen ein. Der Webfilter akzeptiert keine Benutzereinträge.

- **Agent:** Wählen Sie diese Option, um den Sophos Authentication Agent (SAA) zu verwenden. Um den Webfilter verwenden zu können, müssen Benutzer zunächst den Agent ausführen und sich authentifizieren.
- **Apple OpenDirectory SSO:** Wählen Sie diese Option, wenn Sie *LDAP* auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Server* konfiguriert haben und Sie Apple OpenDirectory verwenden. Damit der Proxy richtig funktioniert, müssen Sie zusätzlich eine MAC OS X Single Sign-On Kerberos-Schlüsseldatei auf der Registerkarte *Web Protection* > *Webfilter* > *Erweitert* hochladen. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.Beachten Sie, dass der Safari-Browser SSO nicht unterstützt.

- **Einfache Benutzerauthentifizierung:** In diesem Modus muss sich jeder Client gegenüber dem Proxy authentifizieren, bevor er ihn verwendet. Weitere Informationen zu den unterstützten Authentifizierungsmethoden finden Sie unter *Definitionen & Benutzer* > *Authentifizierungsdienste*. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.
- **eDirectory SSO:** Wählen Sie diese Option, wenn Sie *eDirectory* auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste > Server* konfiguriert haben. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

Hinweis – Für die Modi eDirectory und Active Directory Single Sign-On (SSO) speichert der Webfilter die IP-Adressen und Zugangsdaten der anfragenden Clients bis zu fünfzehn Minuten; für Apple OpenDirectory SSO speichert er nur die Gruppeninformationen. Das Zwischenspeichern reduziert die Last auf den Authentifizierungsservern, aber es bedeutet auch, dass es bis zu fünfzehn Minuten dauern kann, bis Änderungen an Benutzern, Gruppen oder dem Anmeldestatus der zugreifenden Benutzer vom Webfilter berücksichtigt werden.

- **Transparenzmodus:** Im Transparenzmodus werden alle Verbindungen von Client-Browseranwendungen auf Port `80` (bzw. Port `443`, wenn SSL aktiviert ist) abgefangen und ohne clientseitige Konfiguration an den Webfilter weitergeleitet. Der Client merkt dabei vom Webfilter nichts. Der Vorteil dieses Modus ist, dass keine zusätzliche Verwaltung oder clientseitige Konfiguration nötig ist; der Nachteil ist, dass nur HTTP-Anfragen (Port 80) verarbeitet werden können. Deshalb werden die Proxy-Einstellungen im Client-Browser unwirksam, wenn Sie Transparent als Modus wählen.

Hinweis – Im Transparenzmodus entfernt der Webfilter NTLM-Authentifizierungsheader von HTTP-Anfragen. Darüber hinaus kann der Webfilter keine FTP-Anfragen in diesem Modus verarbeiten. Wenn Ihre Clients auf solche Dienste zugreifen wollen, müssen Sie den Port (`21`) in der Firewall öffnen. Beachten Sie auch, dass manche Webserver einige Daten über einen anderen Port als Port 80 übermitteln, insbesondere Streaming-Video- und -Audiodaten. Diese Anfragen werden nicht beachtet, wenn der Webfilter im

Transparenzmodus arbeitet. Um solchen Verkehr zu unterstützen, müssen Sie entweder einen anderen Modus wählen oder eine explizite Firewallregel anlegen, die diesen Verkehr erlaubt.

Volltransparent (optional): Wählen Sie die Option, um die Quell-IP der Clients zu erhalten, anstatt sie durch die IP des Gateways zu ersetzen. Das ist nützlich, wenn Ihre Clients öffentliche IP-Adressen verwenden, die nicht durch den Webfilter verschleiert werden sollen. Diese Option ist nur im Bridge-Modus verfügbar, da sie nur dort sinnvoll ist.

Wählen Sie eine Authentifizierungsmethode aus:

- **Keine:** Wählen Sie diese Option, wenn keine Authentifizierung verwendet werden soll.
- **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

  Hinweis – Wenn Sie eine Active-Directory-Benutzergruppe anlegen, empfehlen wir dringend, im Feld *Active-Directory-Gruppen* die Namen der Active-Directory-Gruppen oder Benutzer direkt manuell einzugeben, statt die LDAP-Strings zu verwenden. Beispiel: Statt eines LDAP-Strings `CN=ads_group1,CN=Users,DC=example,DC=com` geben Sie einfach den Namen `ads_group1` ein.

  Hinweis – Wenn Sie Kerberos verwenden, geben Sie in das Feld *Active-Directory-Gruppen* nur Gruppen ein. Der Webfilter akzeptiert keine Benutzereinträge.

- **Agent:** Wählen Sie diese Option, um den Sophos Authentication Agent (SAA) zu verwenden. Um den Webfilter verwenden zu können, müssen Benutzer zunächst den Agent ausführen und sich authentifizieren. Sie kön-

nen im Feld *Zugelassene Benutzer/Gruppen* Benutzer und/oder Gruppen auswählen oder anlegen, die den Webfilter verwenden dürfen.

- **Browser:** Wenn Sie diese Funktion wählen, wird den Benutzern in ihrem Browser ein Dialogfenster zur Anmeldung angezeigt, über das sie sich beim Webfilter authentifizieren können. Dieser Modus ermöglicht die Benutzernamen-basierte Verfolgung (engl. tracking), Berichterstellung und Surfen ohne clientseitige Browserkonfiguration. Darüber hinaus können Sie Nutzungsbedingungen einrichten, die dann zusätzlich auf der Anmeldeseite angezeigt werden und von den Benutzern akzeptiert werden müssen, bevor sie fortfahren können. Weitere Informationen zu Nutzungsbedingungen finden Sie im Kapitel *Verwaltung > Anpassungen > Web-Meldungen*.

Wählen Sie „Gerätespezifische Authentifizierung aktivieren“, um die Authentifizierung nach Gerät zu kontrollieren. Anschließend können Sie auf das Plussymbol klicken und Geräte hinzufügen sowie die Authentifizierungsmethode für diese Geräte auswählen.

5. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Wichtiger Hinweis – Wenn SSL-Scanning zusammen mit dem Transparenzmodus aktiviert ist, werden einige SSL-Verbindungen nicht zustande kommen, z. B. SSL-VPN-Tunnel. Um SSL-VPN-Verbindungen zu ermöglichen, fügen Sie den entsprechenden Zielhost zur Liste *Transparenzmodus-Ausnahmen* hinzu (siehe *Web Protection > Filteroptionen > Sonstiges*). Um darüber hinaus Zugang zu Hosts mit einem selbstsignierten Zertifikat zu haben, müssen Sie eine Ausnahme für diese Hosts anlegen und die Option *Zertifikat-Vertrauensprüfung* auswählen. Der Proxy wird deren Zertifikate dann nicht überprüfen.

Live-Protokoll

Das Webfilter-Live-Protokoll stellt Informationen zu Webanfragen bereit.Klicken Sie auf die Schaltfläche *Live-Protokoll öffnen*, um das Webfilter-Live-Protokoll in einem neuen Fenster zu öffnen.

9.1.3 Richtlinien

Verwenden Sie zur Erstellung und Verwaltung von Webfilter-Richtlinienzuweisungen die Registerkarte *Web Protection > Webfilter > Richtlinien*. Standardmäßig ist die Basisrichtlinie im

unteren Bereich der Registerkarte *Richtlinien* aufgeführt. Richtlinien werden der Reihe nach von oben nach unten durchgesetzt. Wenn keine Richtlinie ausgelöst wird, gilt die Basisrichtlinie.

Um eine neue Richtlinie zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf das Plussymbol in der rechten oberen Ecke.**
   Das Dialogfeld *Richtlinie hinzufügen* wird angezeigt.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Richtlinie ein.

   Benutzer/Gruppen: Wählen Sie Benutzer oder Benutzergruppen aus oder fügen Sie neue Benutzer hinzu, die der Richtlinie zugewiesen werden sollen. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

   Erweiterte Einstellungen: Wenn Sie *Diese Richtlinie auf Anfragen anwenden, die aufgrund einer Ausnahme die Authentifizierung übersprungen haben* auswählen, wird die Richtlinie auf Elemente angewendet, die auf der Seite *Filteroptionen > Ausnahmen* von der Authentifizierung ausgenommen wurden.

   Zeit-Ereignis: Die Richtlinie gilt für den von Ihnen ausgewählten Zeitraum.Wählen Sie *Immer* , damit die Richtlinie jederzeit aktiv ist. Zeitraumdefinitionen werden auf der Registerkarte *Definitionen & Benutzer > Zeitraumdefinitionen* verwaltet.

   Filteraktion: Wählen Sie eine vorhandene Filteraktion aus oder klicken Sie auf das Plussymbol, um im Filteraktionsassistenten eine neue zu erstellen. Es gibt eine *Standard-Filteraktion* , die Sie bearbeiten können. Oder erstellen Sie eine neue Filteraktion. Eine Filteraktion legt fest, welche Sicherheitsmerkmale für eine Richtlinie gelten.Filteraktionen können außerdem auf der Registerkarte *Webfilter-Profile > Filteraktionen* verwaltet werden.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Richtlinie wird ganz oben in der Liste *Richtlinien* angezeigt.

4. **Aktivieren Sie die Richtlinie.**
   Die neue Richtlinie ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Richtlinie zu aktivieren. Die Richtlinie ist jetzt aktiv (Schieberegler ist grün).

- Zum Bearbeiten einer Richtlinie klicken Sie auf ihren Namen.
- Um die Reihenfolge zu ändern, in der Richtlinien ausgeführt werden, bewegen Sie Richtlinien in der Liste mithilfe des Aufwärts- oder Abwärtspfeils auf der rechten Seite nach oben oder unten.
- Zum Bearbeiten einer Filteraktion klicken Sie auf den Namen der Filteraktion, um den Assistenten *Filteraktion bearbeiten* anzuzeigen, oder wechseln Sie zur Registerkarte *Webfilter-Profile* > *Filteraktionen*.

9.1.3.1 Filteraktionsassistent

Der Assistent *Filteraktion hinzufügen/bearbeiten* dient zum Erstellen oder Bearbeiten von Filteraktionen zur Verwendung in Ihren Web-Richtlinien. Sie können den Assistenten über die Dialogfelder *Richtlinie hinzufügen* oder *Richtlinie bearbeiten* starten oder indem Sie auf den Namen einer vorhandenen Filteraktion auf der Registerkarte *Webfilter* > *Richtlinien* klicken.

Sie können Ihre Filteraktionen auch auf der Registerkarte *Webfilter-Profil* > *Filteraktionen* verwalten. Dort können Sie Filteraktionen hinzufügen, bearbeiten, klonen oder löschen. Jetzt aber können Sie zudem den Assistenten *Filteraktion hinzufügen/bearbeiten* auf der Registerkarte *Webfilter* > *Richtlinien* zum Erstellen, Bearbeiten und Zuweisen von Filteraktionen verwenden.

9.1.3.2 Kategorien

Konfigurieren Sie Standardeinstellungen, um den Zugriff auf bestimmte Arten von Websites zu steuern.

Name: Geben Sie einen aussagekräftigen Namen für diese Filteraktion ein.

***Zulassen/Blockieren*-Auswahl:** Legen Sie fest, ob Ihre Auswahl von Website-Kategorien zugelassen oder blockiert werden soll. Die folgenden Optionen sind möglich:

- **Inhalt zulassen, der die unten stehenden Kriterien nicht erfüllt:** Blockieren Sie nur die Kategorien, die Sie ausgewählt haben.
- **Inhalt blockieren, der die unten stehenden Kriterien nicht erfüllt:** Blockieren Sie alle Kategorien, außer denen, die Sie ausgewählt haben.

Die Standardoption ist *Zulassen*. Die Liste der Kategorien zeigt, ob die ausgewählten Kategorien zugelassen oder blockiert werden. In Fällen, in denen mehr als eine Kategorie auf eine Website zutrifft, muss die Option auf beide zutreffen.Wenn Sie beispielsweise Unterhaltung zulassen, aber Spiele blockieren, würde eine Website, die in beide Kategorien eingeordnet

wird, zugelasen werden, wenn die Schaltfläche *Zulassen* ausgewählt wird, und blockiert werden, wenn die Schaltfläche *Blockieren* ausgewählt wird.

Hinweis – Um auf die Kategorisierungsdatenbank zugreifen zu können, müssen die TCP-Ports `6000` oder `80` in Upstream-Firewalls offen sein. Wenn ein übergeordneter Proxy (Parent-Proxy) konfiguriert ist, werden alle Anfragen an die Datenbank über den übergeordneten Proxy geleitet.

Spyware-Infizierung und -Kommunikation blockieren: Bei Auswahl dieser Option wird Spyware erkannt und blockiert. Darüber hinaus entdeckt und blockiert diese Funktion Verkehr, der von installierten Spyware-Programmen ausgeht.Beachten Sie, dass diese Option nur verfügbar ist, wenn die erste Option auf dieser Seite auf *Zulassen* gestellt ist.

Hinweis – Die Kategorie Spyware kann keiner der 18 verfügbaren Gruppen zugeordnet werden, deshalb kann sie nur durch die Option *Spyware-Infizierung und -Kommunikation blockieren* aktiviert werden.

Kategorien: Konfigurieren Sie für die Website-Kategorien *Blockieren*, *Zulassen* oder *Warnen*.Website-Kategorien und ihre zugehörigen Unterkategorien können auf der Registerkarte *Web Protection > Filteroptionen > URL-Filterkategorien* konfiguriert werden.Wenn Sie die Aktion *Warnen* auswählen, wird Benutzern, die eine Website dieser Kategorie aufrufen, zunächst eine Warnseite angezeigt, aber sie können trotzdem fortfahren und die Seite aufrufen.

Unkategorisierte Websites: Sie können als Standardaktion für unkategorisierte Websites *Blockieren*, *Warnen* oder *Zulassen* konfigurieren.

Websites blockieren, deren Ruf schlechter als dieser Schwellenwert ist: Websites können in folgende Kategorien unterteilt werden: *Vertrauenswürdig*, *Neutral*, *Unüberprüft*, *Verdächtig* oder schädlich, wobei letztere nicht aufgeführt wird.Unklassifizierte Websites werden als *Unüberprüft* (engl. unverified) eingestuft. Sie können wählen, welchen Ruf eine Website haben muss, um für Ihr Netzwerk erreichbar zu sein. Websites unterhalb des gewählten Schwellenwerts werden blockiert.Beachten Sie, dass diese Option nur verfügbar ist, wenn die erste Option auf dieser Seite auf *Zulassen* gestellt ist.Weitere Informationen zum Ruf von Websites finden Sie unter http://www.trustedsource.org.

Klicken Sie auf *Weiter*, um zur nächsten Konfigurationsseite zu wechseln, auf *Speichern*, um Ihre Konfiguration zu speichern, oder auf *Abbrechen*, um alle Änderungen zu verwerfen und das Konfigurationsdialogfeld zu schließen.

9.1.3.3 Websites

Diese Websites blockieren: Wenn Sie eine bestimmte URL oder Website blockieren möchten, oder eine Auswahl von Webseiten einer bestimmten Domäne, unabhängig von ihrer Kategorie, legen Sie diese hier fest. Das bewirkt, dass hier definierte Websites blockiert werden können, selbst wenn sie zu einer Kategorie gehören, die Sie zulassen.

1. **Klicken Sie auf das Plussymbol, um das Dialogfenster *Whitelist-/Blacklist-Objekt hinzufügen* zu öffnen.**
2. **Nehmen Sie die folgenden Einstellungen vor:**
   - **Name:** Geben Sie einen aussagekräftigen Namen für das Regulärer-Ausdruck-Objekt ein.
   - **Basis für URL-Abgleich: Domänen:** Geben Sie die Domänen ein, für die Sie alle oder bestimmte Webseiten blockieren möchten. Sie müssen den ganzen Domänennamen eingeben, einschließlich z. B. `www`. Webseiten der festgelegten Domänen werden blockiert, wenn einer der unten definierten regulären Ausdrücke auf die URL zutrifft. Wenn kein regulärer Ausdruck angegeben ist, wird die gesamte Domäne blockiert.
   - **Basis für URL-Abgleich: Regulärer Ausdruck:** Geben Sie die regulären Ausdrücke ein, die Sie für die oben festgelegten Domänen verbieten möchten. Wenn oben keine Domäne angegeben ist, wird der reguläre Ausdruck auf alle Domänen angewendet. Beachten Sie, dass ein regulärer Ausdruck sowohl mit der URL als auch mit Suchergebnissen oder Teilen ähnlicher URLs übereinstimmen kann, was zu unbeabsichtigten Blockierungen führen kann. Um den Abgleich Ihres regulären Ausdrucks auf bestimmte Domänen zu beschränken, wählen Sie *Abgleich nur für diese Domänen durchführen* und fügen Sie Domänen hinzu.

     Querverweis – Detaillierte Informationen zur Verwendung von regulären Ausdrücken finden Sie in der Sophos-Knowledgebase.

     Hinweis – Sie sollten die Webseiten so präzise wie möglich definieren. Das Verwenden von regulären Ausdrücken ohne Angabe von Domänen kann sich negativ auf die Leistung auswirken.

   - **Kommentar** (optional): Fügen Sie eine Beschreibung oder sonstige Infor-

mationen hinzu.

3. **Klicken Sie auf *Speichern*.**

Diese Websites zulassen: Wenn Sie eine bestimmte URL oder Website oder eine Auswahl von Webseiten einer bestimmten Domäne, unabhängig von ihrer Kategorie, zulassen möchten, legen Sie diese hier fest. Das bewirkt, dass hier definierte Websites zugelassen werden können, selbst wenn sie zu einer Kategorie gehören, die Sie blockieren möchten.

1. **Klicken Sie auf das Plussymbol, um das Dialogfenster *Regulärer-Ausdruck-Objekt hinzufügen* zu öffnen.**

2. **Nehmen Sie die folgenden Einstellungen vor:**

   - **Name:** Geben Sie einen aussagekräftigen Namen für das Regulärer-Ausdruck-Objekt ein.

   - **Basis für URL-Abgleich: Domänen:** Geben Sie die Domänen ein, für die Sie alle oder bestimmte Webseiten blockieren möchten. Sie müssen den ganzen Domänennamen eingeben, einschließlich z. B. `www`. Webseiten der festgelegten Domänen werden blockiert, wenn einer der unten definierten regulären Ausdrücke auf die URL zutrifft. Wenn kein regulärer Ausdruck angegeben ist, wird die gesamte Domäne blockiert.

   - **Basis für URL-Abgleich: Regulärer Ausdruck:** Geben Sie die regulären Ausdrücke ein, die Sie für die oben festgelegten Domänen verbieten möchten. Wenn oben keine Domäne angegeben ist, wird der reguläre Ausdruck auf alle Domänen angewendet. Beachten Sie, dass ein regulärer Ausdruck sowohl mit der URL als auch mit Suchergebnissen oder Teilen ähnlicher URLs übereinstimmen kann, was zu unbeabsichtigten Blockierungen führen kann. Um den Abgleich Ihres regulären Ausdrucks auf bestimmte Domänen zu beschränken, wählen Sie *Abgleich nur für diese Domänen durchführen* und fügen Sie Domänen hinzu.

     Querverweis – Detaillierte Informationen zur Verwendung von regulären Ausdrücken finden Sie in der Sophos-Knowledgebase.

     Hinweis – Sie sollten die Webseiten so präzise wie möglich definieren. Das Verwenden von regulären Ausdrücken ohne Angabe von Domänen kann sich negativ auf die Leistung auswirken.

- **Kommentar** (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**

9.1.3.4 Downloads

Konfigurieren Sie, welche Datei- und MIME-Typen blockiert werden sollen oder vor denen gewarnt werden soll.

Dateierweiterungen: Filtern Sie bestimmte Dateien aus dem Internetverkehr mithilfe von Dateierweiterungen in der Liste *Warned Extenstions*. Sie können weitere Dateierweiterungen hinzufügen oder solche Erweiterungen aus der Liste löschen, vor denen nicht gewarnt werden soll. Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Warned Extenstions* und geben die Dateierweiterung ein, die blockiert werden soll, zum Beispiel `exe` (ohne voranstehenden Punkt).

Blockierte Erweiterungen: Filtern Sie bestimmte Dateien aus dem Internetverkehr mithilfe von Dateierweiterungen in der Liste *Blockierte Dateierweiterungen*. Sie können weitere Dateierweiterungen hinzufügen oder solche Erweiterungen aus der Liste löschen, die nicht blockiert werden sollen. Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Blockierte Erweiterungen* und geben die Dateierweiterung ein, die blockiert werden soll, zum Beispiel `exe` (ohne voranstehenden Punkt).

Hinweis – In Archiven (z. B. `zip`-Dateien) gespeicherte Dateien können nicht nach blockierten Dateitypen, blockierten Erweiterungen oder blockierten MIME-Typen durchsucht werden. Wenn Sie Ihr Netzwerk vor diesen in Archiven gespeicherten Dateien schützen möchten, sollten Sie Dateitypen wie zip, rar usw. generell blockieren.

MIME-Typen: Filtern Sie Dateien aus dem Internetverkehr mithilfe von MIME-Typen in der Liste *Warned MIME-Types*. Um einen MIME-Typ hinzuzufügen klicken Sie auf das Plussymbol im Feld *Warned MIME-Types* und geben den MIME-Typ ein. Sie können in der Liste *Warned MIME-Types* Platzhalter (*) verwenden, z. B. `audio/*`.

Blockierte MIME-Typen: Filtern Sie Dateien aus dem Internetverkehr mithilfe von MIME-Typen in der Liste *Blockierte MIME-Typen*. Um einen MIME-Typ hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Blockierte MIME-Typen* und geben den MIME-Typ ein. Sie können in der Liste *Blockierte MIME-Typen* Platzhalter (*) verwenden, z. B. `audio/*`.

Downloads blockieren, die größer sind als: Wählen Sie diese Option, um Benutzer daran zu hindern, Dateien herunterzuladen, die größer sind als die festgelegte Größe (in MB).

Klicken Sie auf *Weiter*, um zur nächsten Konfigurationsseite zu wechseln, auf *Speichern*, um Ihre Konfiguration zu speichern, oder auf *Abbrechen*, um alle Änderungen zu verwerfen und das Konfigurationsdialogfeld zu schließen.

9.1.3.5 Antivirus

Antivirus

Antiviren-Scan verwenden: Wählen Sie diese Option, um eingehenden und ausgehenden Internetverkehr auf Viren zu scannen. Sophos UTM bietet mehrere Antiviren-Mechanismen:

- **Einzelscan:** Standardeinstellung; bietet maximale Leistung. Die auf der Registerkarte *Systemeinstellungen* > *Scan-Einstellungen* festgelegte Engine wird verwendet.
- **Zweifachscan:** Bietet maximale Erkennungsrate, da der entsprechende Verkehr von zwei verschiedenen Virenscannern gescannt wird. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist.
- **Potenziell unerwünschte Anwendungen (PUA) blockieren:** PUA sind Programme, die nicht schädlich, in einer Geschäftsumgebung aber unerwünscht sind. Diese Funktion ist nur bei Verwendung der Sophos Antivirus-Engine verfügbar. Um bestimmte PUA bei aktiver Blockierung dennoch zuzulassen, fügen Sie unter *Web Protection* > *Webfilter* > *Filteroptionen* > *PUAs* Ausnahmen hinzu.

Dateien nicht scannen, die größer sind als: Legen Sie die Maximalgröße von Dateien fest, die von den Antiviren-Engines gescannt werden sollen. Dateien, die größer sind, werden nicht gescannt.

Tipp – Um zu verhindern, dass Dateien mit einer Dateigröße über der maximalen Scangröße heruntergeladen werden, legen Sie den Wert *Downloads ab dieser Größe blockieren* auf der Seite *Downloads* entsprechend fest.

Entfernen von aktivem Inhalt

Im Abschnitt *Entfernen von aktivem Inhalt* können Sie einstellen, dass spezifischer Internetinhalt, wie auf Webseiten eingebettete Objekte, automatisch entfernt wird. Sie können die folgenden Einstellungen konfigurieren:

- **Javascript deaktivieren:** Mit dieser Funktion werden alle `<SCRIPT>`-Tags aus HTML-Seiten entfernt, wodurch Funktionen deaktiviert werden, die in HTML-Seiten eingebettet

oder eingebunden sind.

- **Eingebettete Objekte entfernen (ActiveX/Java/Flash):** Durch diese Funktion werden alle `<OBJECT>`-Tags aus HTML-Seiten entfernt, wodurch dynamische Inhalte wie ActiveX, Flash oder Java aus dem eingehenden HTTP-Verkehr gelöscht werden.

Klicken Sie auf *Weiter*, um zur nächsten Konfigurationsseite zu wechseln, auf *Speichern*, um Ihre Konfiguration zu speichern, oder auf *Abbrechen*, um alle Änderungen zu verwerfen und das Konfigurationsdialogfeld zu schließen.

9.1.3.6 Zusätzliche Optionen

Website-Sicherheitsfunktionen erzwingen

SafeSearch: Manche Suchmaschinenanbieter haben eine SafeSearch-Funktion, die Erwachseneninhalte aus den Suchergebnissen entfernt. Sie können die Nutzung von SafeSearch für Google, Bing und Yahoo erzwingen. Wenn diese Option aktiviert ist, wird SafeSearch für diesen Anbieter erzwungen und kann von Webfilter-Benutzern weder deaktiviert noch umgangen werden. Um die Funktion zu konfigurieren, wählen Sie den Anbieter aus, für den SafeSearch erzwungen werden soll.

YouTube für Schulen: Wenn diese Option aktiviert ist, können Benutzer nur auf YouTube-Videos aus dem Bereich YouTube EDU oder solche, die über Ihr Schulkonto hochgeladen wurden, zugreifen. Dazu müssen Sie sich beim Programm „YouTube für Schulen“ anmelden. Sie erhalten dann eine Schul-ID, die Sie unten eingeben müssen.

Hinweis – Auf der Sophos UTM müssen Sie sicherstellen, dass die Top-Level-Domänen `youtube.com` und `ytimg.com` sowie Videos im Allgemeinen nicht blockiert werden. Wenn Sie *YouTube für Schulen* aktiviert haben, müssen Sie die Schul-ID oder den Code eingeben, den Sie von YouTube erhalten haben.

Zulässige Domänen für Google Apps erzwingen: Google Apps kann Benutzern den Zugriff auf bestimmte Dienste verwehren, wenn ihr Google-Konto kein Mitglied der Google Apps-Domäne ist. Wenn diese Option ausgewählt wird, ist die Funktion aktiviert und kann von Webfilterbenutzern nicht ausgeschaltet oder umgangen werden. Wählen Sie *Zulässige Domänen für Google Apps erzwingen* aus, um die Funktion zu konfigurieren. Klicken Sie dann oben im Feld *Domänen* auf das Plus- oder das Aktionssymbol, um Google Apps-Domänen hinzuzufügen oder zu importieren.

Aktivitätsprotokollierung

Sie können festlegen, welche Aktivitäten protokolliert werden:

- **Besuchte Seiten protokollieren:** Mit dieser Funktion werden Informationen über alle Seiten protokolliert, die über UTM besucht wurden.
- **Blockierte Seiten protokollieren:** Mit dieser Funktion werden Informationen über Seiten protokolliert, für die der Zugriff blockiert wurde.

Netzwerkkonfiguration

Sie können übergeordnete Proxies konfigurieren (sowohl global als auch profilbasiert; siehe *Web Protection > Filteroptionen > Übergeordnete Proxies*).

Hinweis – HTTPS-Anfragen im Transparenzmodus sind mit aktivierten übergeordneten Proxies *nicht* möglich,wenn SSL-Scanning aktiviert ist.

Um einen übergeordneten Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf das Plussymbol über der Liste übergeordneter Proxies.**
   Das Dialogfeld *Übergeordneten Proxy hinzufügen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**

   Name: Geben Sie einen aussagekräftigen Namen für den übergeordneten Proxy ein.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

   Proxy für diese Hosts verwenden: Fügen Sie Hosts zu diesem Feld hinzu, für die ein übergeordneter Proxy verwendet werden soll, z. B. `*.wikipedia.org`. Sie können hier musterbasierte Suchausdrücke (Pattern Matching) verwenden. Reguläre Ausdrücke sind hingegen nicht zugelassen. Wenn Sie das Feld leer lassen, wird, sobald Sie *Speichern* anklicken, automatisch ein Asterisk (*) hinzugefügt, der alle Hosts umfasst. Eine solche Proxy-Definition kann daher als Ersatzproxy angesehen werden, der greift, wenn keiner der anderen eventuell vorhandenen Proxys die Bedingungen erfüllt.

   Übergeordneter Proxy: Wählen Sie die Netzwerkdefinition des übergeordneten Proxys aus oder fügen Sie sie hinzu.

   Port: Der Standardport für die Verbindung zum übergeordneten Proxy ist 8080. Wenn Ihr übergeordneter Proxy einen anderen Port erfordert, können Sie diesen hier ändern.

Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, aktivieren Sie das Auswahlkästchen und geben Sie den Benutzernamen und das Kennwort hier ein.

3. **Klicken Sie auf *Speichern*.**
   Der neue übergeordnete Proxy wird in der Liste *Übergeordnete Proxies* und auf der Seite *Web Protection > Filteroptionen > Übergeordnete Proxies* angezeigt.

Um einen übergeordneten Proxy zu bearbeiten oder zu löschen, klicken Sie auf den Namen des Proxys.

Klicken Sie auf *Speichern*, um Ihre Konfiguration zu speichern, oder auf *Abbrechen*, um alle Änderungen zu verwerfen und das Konfigurationsdialogfeld zu schließen.

9.2 Webfilter-Profile

Sophos UTMverfügt über einen Webfilter, der dafür ausgelegt und optimiert ist zu kontrollieren, welche Internetinhalte für welchen Teil des Netzwerks zugänglich sind. Dadurch hindert er Benutzer daran, Inhalte zu sehen, die Sie ablehnen. Sie können den Webfilter so konfigurieren, dass er ausgewählte Netzwerke global überwacht. Alternativ dazu können Sie individuelle Webfilter-Profile anlegen, die verwendet werden können, um verschiedene Sicherheitsrichtlinien auf verschiedene Netzwerksegmente anzuwenden. Auf diese Weise können Sie unterschiedliche Richtlinien für die verschiedenen Abteilungen innerhalb Ihres Unternehmens definieren, sogar mit unterschiedlichen Benutzerauthentifizierungsmethoden.

9.2.1 Filterprofile

Filterprofile können zur Erstellung verschiedener Inhaltsfilter-Richtlinien verwendet werden und ermöglichen es Ihnen, auf unterschiedliche Adressen Ihres Netzwerks unterschiedliche Richtlinien anzuwenden. So können Sie verschiedene Richtlinien für unterschiedliche Abteilungen in Ihrem Unternehmen definieren. Zusätzlich kann jedem Filterprofil seine eigene Methode zur Benutzerauthentifizierung zugewiesen werden.

Um ein Filterprofil anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf das Plussymbol in der rechten oberen Ecke.**
   Der Assistent *Profil hinzufügen* wird geöffnet.

2. **Geben Sie einen *Namen* und einen *Kommentar* ein.**

3. **Wählen Sie die zugelassenen Netzwerke aus.**
   Wählen Sie die Netzwerke aus, die den Webfilter verwenden dürfen. Der Webfilter wartet standardmäßig auf Anfragen an TCP -Port `8080` und lässt jeden Client zu, der sich in einem Netzwerk befindet, das im Feld *Zugelassene Netzwerke* aufgeführt ist.

4. **Wählen Sie die zugelassenen Endpoint-Gruppen aus.**
   Wenn Endpoint Web Control aktiviert ist, wählen Sie die Endpoint-Gruppen aus, die den Webfilter verwenden können sollen.

5. **HTTPS-Verkehr (SSL):**
   Um SSL-Verkehr zu scannen wählen Sie aus den folgenden Optionen aus:

   - **Nicht scannen:** Diese Option ist nur im Transparenzmodus verfügbar. Wenn diese Option ausgewählt ist geht kein HTTPS-Verkehr durch den Proxy und wird nicht gescannt.
   - **Nur URL-Filterung:** Diese Option führt URL-Kategorie und Reputationsprüfungen aus, scannt aber nicht die Inhalte des HTTPS-Verkehrs.
   - **Entschlüsseln und scannen:** Wählen Sie diese Option um die komplette Überprüfung für den HTTPS-Verkehr durchzuführen.

6. **Wählen Sie einen Betriebsmodus aus:**
   Falls Sie einen Betriebsmodus mit Benutzerauthentifizierung wählen, sollten Sie auch die Benutzer und Gruppen angeben, die auf den Webfilter zugreifen dürfen. Die folgenden Betriebsmodi sind möglich:

   - **Standardmodus:** Im Standardmodus lauscht der Webfilter standardmäßig auf Client-Anfragen auf Port 8080 und lässt jeden Client zu, der sich in einem Netzwerk befindet, das im Feld Zugelassene Netzwerke aufgeführt ist. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.
     Wählen Sie die Standard-Authentifizierungsmethode aus.

     - **Keine:** Wählen Sie diese Option, wenn keine Authentifizierung verwendet werden soll.
     - **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste >Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der Webfilter in der Browser-

Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

Hinweis – Wenn Sie eine Active-Directory-Benutzergruppe anlegen, empfehlen wir dringend, im Feld *Active-Directory-Gruppen* die Namen der Active-Directory-Gruppen oder Benutzer direkt manuell einzugeben, statt die LDAP-Strings zu verwenden. Beispiel: Statt eines LDAP-Strings `CN=ads_group1,CN=Users,DC=example,DC=com` geben Sie einfach den Namen `ads_group1` ein.

Hinweis – Wenn Sie Kerberos verwenden, geben Sie in das Feld *Active-Directory-Gruppen* nur Gruppen ein. Der Webfilter akzeptiert keine Benutzereinträge.

- **Agent:** Wählen Sie diese Option, um den Sophos Authentication Agent (SAA) zu verwenden. Um den Webfilter verwenden zu können, müssen Benutzer zunächst den Agent ausführen und sich authentifizieren.
- **Apple OpenDirectory SSO:** Wählen Sie diese Option, wenn Sie *LDAP* auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Server* konfiguriert haben und Sie Apple OpenDirectory verwenden. Damit der Proxy richtig funktioniert, müssen Sie zusätzlich eine MAC OS X Single Sign-On Kerberos-Schlüsseldatei auf der Registerkarte *Web Protection* > *Filteroptionen* > *Sonstiges* hochladen. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.Beachten Sie, dass der Safari-Browser SSO nicht unterstützt.
- **Einfache Benutzerauthentifizierung:** In diesem Modus muss sich jeder Client gegenüber dem Proxy authentifizieren, bevor er ihn verwendet. Weitere Informationen zu den unterstützten Authentifizierungsmethoden finden Sie unter *Definitionen & Benutzer* > *Authentifizierungsdienste*. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.
- **Browser:** Wenn Sie diese Funktion wählen, wird den Benutzern in ihrem Browser ein Dialogfenster zur Anmeldung angezeigt, über das sie sich beim Webfilter authentifizieren können. Dieser Modus ermöglicht die Benutzernamen-basierte Verfolgung (engl. tracking), Berichterstellung und Surfen ohne Client-seitige Browserkonfiguration. Darüber hinaus können Sie Nutzungsbedingungen einrichten, die dann zusätzlich auf der Anmeldeseite

angezeigt werden und von den Benutzern akzeptiert werden müssen, bevor sie fortfahren können. Weitere Informationen zu Nutzungsbedingungen finden Sie im Kapitel *Verwaltung > Anpassungen > Web-Meldungen*.

- **eDirectory SSO:** Wählen Sie diese Option, wenn Sie *eDirectory* auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste > Server* konfiguriert haben. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

Hinweis – Für die Modi eDirectory und Active Directory Single Sign-On (SSO) speichert der Webfilter die IP-Adressen und Zugangsdaten der anfragenden Clients bis zu fünfzehn Minuten; für Apple OpenDirectory SSO speichert er nur die Gruppeninformationen. Das Zwischenspeichern reduziert die Last auf den Authentifizierungsservern, aber es bedeutet auch, dass es bis zu fünfzehn Minuten dauern kann, bis Änderungen an Benutzern, Gruppen oder dem Anmeldestatus der zugreifenden Benutzer vom Webfilter berücksichtigt werden.

Wenn Sie einen Authentifizierungsmodus wählen der Benutzerauthentifizierung erfordert, wählen Sie *Zugang bei Authentifizierungsfehler blockieren* aus um Benutzern den Zugriff zu verweigern, deren Authentifizierung fehlgeschlagen ist.

- **Transparenzmodus:** Im Transparenzmodus werden alle Verbindungen von Client-Browseranwendungen auf Port `80` (bzw. Port `443`, wenn SSL aktiviert ist) abgefangen und ohne clientseitige Konfiguration an den Webfilter weitergeleitet. Der Client merkt dabei vom Webfilter nichts. Der Vorteil dieses Modus ist, dass keine zusätzliche Verwaltung oder clientseitige Konfiguration nötig ist; der Nachteil ist, dass nur HTTP-Anfragen (Port 80) verarbeitet werden können. Deshalb werden die Proxy-Einstellungen im Client-Browser unwirksam, wenn Sie Transparent als Modus wählen.

Hinweis – Im Transparenzmodus entfernt der Webfilter NTLM-Authentifizierungsheader von HTTP-Anfragen. Darüber hinaus kann der Webfilter keine FTP-Anfragen in diesem Modus verarbeiten. Wenn Ihre Clients auf solche Dienste zugreifen wollen, müssen Sie den Port (`21`) in der Firewall öffnen. Beachten Sie auch, dass manche Webserver einige Daten über einen anderen Port als Port 80 übermitteln, insbesondere Streaming-Video- und -Audiodaten. Diese Anfragen werden nicht beachtet, wenn der Webfilter im

Transparenzmodus arbeitet. Um solchen Verkehr zu unterstützen, müssen Sie entweder einen anderen Modus wählen oder eine explizite Firewallregel anlegen, die diesen Verkehr erlaubt.

- **Keine:** Wählen Sie diese Option, wenn keine Authentifizierung verwendet werden soll.
- **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste >Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

  Hinweis – Wenn Sie eine Active-Directory-Benutzergruppe anlegen, empfehlen wir dringend, im Feld *Active-Directory-Gruppen* die Namen der Active-Directory-Gruppen oder Benutzer direkt manuell einzugeben, statt die LDAP-Strings zu verwenden. Beispiel: Statt eines LDAP-Strings `CN=ads_group1,CN=Users,DC=example,DC=com` geben Sie einfach den Namen `ads_group1` ein.

  Hinweis – Wenn Sie Kerberos verwenden, geben Sie in das Feld *Active-Directory-Gruppen* nur Gruppen ein. Der Webfilter akzeptiert keine Benutzereinträge.

- **Agent:** Wählen Sie diese Option, um den Sophos Authentication Agent (SAA) zu verwenden. Um den Webfilter verwenden zu können, müssen Benutzer zunächst den Agent ausführen und sich authentifizieren. Sie können im Feld *Zugelassene Benutzer/Gruppen* Benutzer und/oder Gruppen auswählen oder anlegen, die den Webfilter verwenden dürfen.
- **Browser:** Wenn Sie diese Funktion wählen, wird den Benutzern in ihrem Browser ein Dialogfenster zur Anmeldung angezeigt, über das sie sich beim Webfilter authentifizieren können. Dieser Modus ermöglicht die Benutzernamen-basierte Verfolgung (engl. tracking), Berichterstellung und Surfen ohne Client-seitige Browserkonfiguration. Darüber hinaus können Sie Nutzungsbedingungen einrichten, die dann zusätzlich auf der Anmeldeseite

angezeigt werden und von den Benutzern akzeptiert werden müssen, bevor sie fortfahren können. Weitere Informationen zu Nutzungsbedingungen finden Sie im Kapitel *Verwaltung > Anpassungen > Web-Meldungen*.

- **Volltransparent** (optional): Wählen Sie die Option, um die Quell-IP der Clients zu erhalten, anstatt sie durch die IP des Gateways zu ersetzen. Das ist nützlich, wenn Ihre Clients öffentliche IP-Adressen verwenden, die nicht durch den Webfilter verschleiert werden sollen. Diese Option ist nur im Bridge-Modus verfügbar, da sie nur dort sinnvoll ist.

  Wählen Sie die Standard-Authentifizierungsmethode aus:

  - **Keine:** Wählen Sie diese Option, wenn keine Authentifizierung verwendet werden soll.
  - **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Definitionen & Benutzer > Authentifizierungsdienste >Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der Webfilter in der Browser-Konfiguration jedes Clients als HTTP-Proxy angegeben sein.

    Hinweis – Wenn Sie eine Active-Directory-Benutzergruppe anlegen, empfehlen wir dringend, im Feld *Active-Directory-Gruppen* die Namen der Active-Directory-Gruppen oder Benutzer direkt manuell einzugeben, statt die LDAP-Strings zu verwenden. Beispiel: Statt eines LDAP-Strings `CN=ads_group1,CN=Users,DC=example,DC=com` geben Sie einfach den Namen `ads_group1` ein.

    Hinweis – Wenn Sie Kerberos verwenden, geben Sie in das Feld *Active-Directory-Gruppen* nur Gruppen ein. Der Webfilter akzeptiert keine Benutzereinträge.

  - **Agent:** Wählen Sie diese Option, um den Sophos Authentication Agent (SAA) zu verwenden. Um den Webfilter verwenden zu können, müssen Benutzer zunächst den Agent ausführen und sich authentifizieren. Sie kön-

nen im Feld *Zugelassene Benutzer/Gruppen* Benutzer und/oder Gruppen auswählen oder anlegen, die den Webfilter verwenden dürfen.

- **Browser:** Wenn Sie diese Funktion wählen, wird den Benutzern in ihrem Browser ein Dialogfenster zur Anmeldung angezeigt, über das sie sich beim Webfilter authentifizieren können. Dieser Modus ermöglicht die Benutzernamen-basierte Verfolgung (engl. tracking), Berichterstellung und Surfen ohne Client-seitige Browserkonfiguration. Darüber hinaus können Sie Nutzungsbedingungen einrichten, die dann zusätzlich auf der Anmeldeseite angezeigt werden und von den Benutzern akzeptiert werden müssen, bevor sie fortfahren können. Weitere Informationen zu Nutzungsbedingungen finden Sie im Kapitel *Verwaltung > Anpassungen > Web-Meldungen*.

7. **Aktivieren Sie die gerätespezifische Authentifizierung.**
   Um die Authentifizierungsmethode für bestimmte Geräte zu konfigurieren, aktivieren Sie das Auswahlkästchen *Gerätespezifische Authentifizierung aktivieren*. Anschließend können Sie auf das grüne Plussymbol klicken und Gerätetypen sowie die Authentifizierungsmethode auswählen.

8. **Klicken Sie auf *Weiter* oder wählen Sie *Richtlinien* im oberen Bereich des Assistenten.**

9. **Prüfen und erstellen Sie Richtlinien für Ihr Filterprofi.**
   Um eine neue Richtlinie zu erstellen, gehen Sie folgendermaßen vor:
   1. **Klicken Sie auf das Plussymbol in der rechten oberen Ecke.**
      Das Dialogfeld *Richtlinie hinzufügen* wird angezeigt.
   2. **Nehmen Sie die folgenden Einstellungen vor:**
      Name: Geben Sie einen aussagekräftigen Namen für diese Richtlinie ein.

      Benutzer/Gruppen: Wählen Sie Benutzer oder Benutzergruppen aus oder fügen Sie neue Benutzer hinzu, die der Richtlinie zugewiesen werden sollen. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

      Erweiterte Einstellungen: Wenn Sie *Diese Richtlinie auf Anfragen anwenden, die aufgrund einer Ausnahme die Authentifizierung übersprungen haben* auswählen, wird die Richtlinie auf Elemente angewendet, die auf der Seite *Filteroptionen > Ausnahmen* von der Authentifizierung ausgenommen wurden.

Zeit-Ereignis: Die Richtlinie gilt für den von Ihnen ausgewählten Zeitraum.Wählen Sie *Immer* , damit die Richtlinie jederzeit aktiv ist. Zeitraumdefinitionen werden auf der Registerkarte *Definitionen & Benutzer > Zeitraumdefinitionen* verwaltet.

Filteraktion: Wählen Sie eine vorhandene Filteraktion aus oder klicken Sie auf das Plussymbol, um im Filteraktionsassistenten eine neue zu erstellen. Es gibt eine *Standard-Filteraktion* , die Sie bearbeiten können. Oder erstellen Sie eine neue Filteraktion. Eine Filteraktion legt fest, welche Sicherheitsmerkmale für eine Richtlinie gelten.Filteraktionen können außerdem auf der Registerkarte *Webfilter-Profile* > *Filteraktionen* verwaltet werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Richtlinie wird ganz oben in der Liste *Richtlinien* angezeigt.

4. **Aktivieren Sie die Richtlinie.**
   Die neue Richtlinie ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler, um die Richtlinie zu aktivieren. Die Richtlinie ist jetzt aktiv (Schieberegler ist grün).

10. **Klicken Sie auf *Speichern*.**
    Das neue Profil wird in der Liste *Filterprofile* angezeigt.

Wichtiger Hinweis – Wenn SSL-Scanning zusammen mit dem Transparenzmodus aktiviert ist, werden einige SSL-Verbindungen nicht zustande kommen, z. B. SSL-VPN-Tunnel. Um SSL-VPN-Verbindungen zu ermöglichen, fügen Sie den entsprechenden Zielhost zur Liste *Transparenzmodus-Ausnahmen* hinzu (siehe *Web Protection > Filteroptionen > Sonstiges*). Um darüber hinaus Zugang zu Hosts mit einem selbstsignierten Zertifikat zu haben, müssen Sie eine Ausnahme für diese Hosts anlegen und die Option *Zertifikat-Vertrauensprüfung* auswählen. Der Proxy wird deren Zertifikate dann nicht überprüfen.

Zum Bearbeiten oder Löschen eines Filterprofils klicken Sie auf den Namen des Profils in der Liste.

9.2.2 Filteraktionen

Auf der Registerkarte *Webfilter-Profile > Filteraktionen* können Sie eine Auswahl von Konfigurationseinstellungen zu Web Protection anlegen und bearbeiten, mit der verschiedene Schutzarten und Schutzstufen angepasst werden können. Filteraktionen können verschiedenen Benutzern und Benutzergruppen zugewiesen werden und bieten einen flexiblen Weg, den Internetzugriff zu kontrollieren.

Sie können eine neue Filteraktion erstellen, indem Sie auf die Schaltfläche *Neue Filteraktion* klicken, oder eine vorhandene Filteraktion bearbeiten, indem Sie auf die entsprechende Schaltfläche *Bearbeiten* klicken. Durch die Ausführung einer dieser beiden Aktionen wird der Filteraktionsassistent gestartet.Weitere Informationen erhalten Sie unter *Web Protection > Richtlinien > Filteraktionsassistent*.

Auf der Seite *Web Protection > Webfilter-Profile > Filteraktionen* können Sie die Liste der vorhandenen Filteraktionen auch durchsuchen, klonen oder löschen.

9.2.3 Übergeordnete Proxies

Einige Netzwerktopologien erfordern einen Upstream-Web-Proxy-Server.Auf der Registerkarte *Web Protection > Webfilter-Profile > Übergeordnete Proxies* können Sie einen übergeordneten Proxy konfigurieren.

Um einen übergeordneten Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neuer übergeordneter Proxy*.**
   Das Dialogfeld *Neuen übergeordneten Proxy anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diesen übergeordneten Proxy ein.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

   Proxy für diese Hosts verwenden: Fügen Sie Hosts zu diesem Feld hinzu, für die ein übergeordneter Proxy verwendet werden soll, z. B. `*.wikipedia.org`. Sie können hier musterbasierte Suchausdrücke (Pattern Matching) verwenden. Reguläre Ausdrücke sind hingegen nicht zugelassen. Wenn Sie das Feld leer lassen, wird, sobald Sie *Speichern* anklicken, automatisch ein Asterisk (*) hinzugefügt, der alle Hosts umfasst. Eine

solche Proxy-Definition kann daher als Ersatzproxy angesehen werden, der greift, wenn keiner der anderen eventuell vorhandenen Proxys die Bedingungen erfüllt.

Übergeordneter Proxy: Wählen Sie die Netzwerkdefinition des übergeordneten Proxys aus oder fügen Sie sie hinzu.

Port: Der Standardport für die Verbindung zum übergeordneten Proxy ist 8080. Wenn Ihr übergeordneter Proxy einen anderen Port erfordert, können Sie diesen hier ändern.

Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, aktivieren Sie das Auswahlkästchen und geben Sie den Benutzernamen und das Kennwort hier ein.

3. **Klicken Sie auf *Speichern*.**
   Der neue übergeordnete Proxy wird in der Liste *Übergeordnete Proxies* angezeigt.

Der Proxy kann nun in Filteraktionen oder global eingesetzt werden.

Um einen übergeordneten Proxy zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

9.3 Filteroptionen

Auf der Seite *Web Protection > Filteroptionen* können Sie verschiedene Optionen zum Webfilter konfigurieren. Auf den Registerkarten, die von dieser Seite aus zugänglich sind, können Sie u. a. Ausnahmen für Filter, Benutzer, die Filter umgehen können, Filterkategorien sowie HTTPS-Zertifikate und -Instanzen konfigurieren.

9.3.1 Ausnahmen

Auf der Registerkarte *Web Protection > Filteroptionen > Ausnahmen* können Sie Netzwerke, Benutzer/Gruppen und Domänen definieren, die nicht gefiltert/blockiert werden sollen, d. h. auf der Whitelist (Positivliste) stehen. Alle Einträge in den Listen auf dieser Seite sind von bestimmten Web-Protection-Diensten ausgenommen.

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahmenliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Ausnahme ein.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

   Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, die nicht durchgeführt werden sollen:

   - **Authentifizierung:** Wenn der Webfilter im *Authentifizierungsmodus* läuft, können Sie die Authentifizierung für Quellhosts/-netzwerke oder Zieldomänen aussetzen.
   - **Zwischenspeichern:** Wählen Sie diese Option, um die Zwischenspeicherung für spezifische Domänen oder Quellhosts/-netzwerke zu deaktivieren.
   - **Nach Download-Größe blockieren:** Wählen Sie diese Option, um die Blockierung von Inhalt nach Download-Größe zu deaktivieren.
   - **Antivirus:** Wählen Sie diese Option, um die Virenscanfunktion zu deaktivieren, die Nachrichten nach unerwünschten Inhalten wie Viren, Trojanischen Pferden und Ähnlichem durchsucht.
   - **Blockierung von Dateierweiterungen:** Wählen Sie diese Option, um den Dateierweiterungsfilter zu deaktivieren, der Inhalte blockiert, wenn sie bestimmte Dateierweiterungen enthalten.
   - **MIME-Typ-Blockierung:** Wählen Sie diese Option, um den MIME-Typ-Filter zu deaktivieren. Dieser blockiert Inhalte, die einen bestimmten MIME-Typ haben.
   - **URL-Filter:** Wählen Sie diese Option, um den URL-Filter zu deaktivieren, der den Zugriff auf bestimmte Websites kontrolliert.
   - **Inhaltsentfernung:** Wählen Sie diese Option, um die Entfernung von bestimmten Inhalten, wie eingebetteten Objekten (z. B. Multimedia-Dateien) oder JavaScript, auf Webseiten auszulassen.
   - **SSL-Scan:** Wählen Sie diese Option, um das SSL-Scannen der angeforderten Webseite auszulassen. Das ist bei Online-Banking-Websites oder bei Websites sinnvoll, die nicht mit SSL-Überwachung umgehen können. Aus technischen Gründen funktioniert diese Option nicht in Verbindung mit transparenten Webfilter-Modi. Verwenden Sie im Transparenzmodus stattdessen die *Transparenzmodus-Ausnahmen* (siehe Registerkarte Filteroptionen > Sonstiges).Im Standard-Modus können Ausnahmen nur basierend auf dem Zielhost oder der

IP-Adresse gemacht werden, abhängig davon, was der Client übermittelt. Bei Ausnahmen, die auf Kategorien basieren, wird anstelle der ganzen URL nur der Hostname klassifiziert.

- **Zertifikat-Vertrauensprüfung (Trust Check):** Wählen Sie diese Option, um die Vertrauensprüfung für das HTTPS-Server-Zertifikat auszulassen. Beachten Sie, dass das Auslassen der Vertrauensprüfung für das Zertifikat basierend auf einer Übereinstimmung bei Benutzern/Gruppen (*Für alle von diesen Benutzern/Gruppen kommenden Anfragen*) technisch unmöglich ist, wenn der Webfilter im Transparenzmodus mit Authentifizierung arbeitet.
- **Zertifikatsdatumsprüfung:** Wählen Sie diese Option, um die Überprüfung des Zertifikatsdatums auf Gültigkeit auszulassen.

Die beiden folgenden Optionen sind nützlich, wenn es Personen oder Mitglieder z. B. des Betriebsrates gibt, deren Aktivitäten keinesfalls protokolliert werden dürfen:

- **Besuchte Seiten:** Wählen Sie diese Option, um besuchte Seiten nicht zu protokollieren. Diese Seitenanfragen werden auch von der Berichterstellung ausgenommen.
- **Blockierte Seiten:** Wählen Sie diese Option, um Seiten, die blockiert wurden, nicht zu protokollieren. Diese Seitenanfragen werden auch von der Berichterstellung ausgenommen.

Für alle Anfragen: Wählen Sie mindestens eine Bedingung, für die die Sicherheitsprüfungen ausgesetzt werden sollen. Sie können mehrere Bedingungen logisch miteinander verknüpfen, indem Sie entweder *Und* oder *Oder* aus der Auswahlliste vor einer Bedingung auswählen. Die folgenden Bedingungen können konfiguriert werden:

- **Aus diesen Quellnetzwerken:** Wählen Sie diese Option, um Quellhosts/-netzwerke hinzuzufügen, die von Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen.Geben Sie die entsprechenden Hosts oder Netzwerke in das Feld *Hosts/Netzwerke* ein, das nach Auswahl der Bedingung geöffnet wird.
- **Von diesen Quell-Endpointgruppen:** Wählen Sie diese Option, um Computergruppen hinzuzufügen (siehe Registerkarte *Endpoint Protection* > *Computerverwaltung* > *Gruppen verwalten*), die von Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Tragen Sie die entsprechenden Gruppen in das Feld *Quell-Endpointgruppen* ein, das nach Auswahl der Bedingung geöffnet wird.

- **Diese URLs betreffend:** Wählen Sie diese Option, um Zieldomänen hinzufügen, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Fügen Sie die entsprechenden Domänen zum Feld *Zieldomänen* hinzu, das nach Auswahl der Bedingung geöffnet wird. Hier sind reguläre Ausdrücke erlaubt. Beispiel: `^https?://[^.]*\.domain.com`deckt HTTP(S)-Verbindungen zu allen Subdomänen dieser Domäne ab.

  > **Querverweis –** Detaillierte Informationen zur Verwendung von regulären Ausdrücken finden Sie in der Sophos-Knowledgebase.

  > **Hinweis –** Wenn Sie den *Transparenzmodus* verwenden und SSL-Scan aktiviert ist, müssen Sie die Zieldomäne(n) als IP-Adresse(n) angeben. Andernfalls wird die Ausnahme aus technischen Gründen fehlschlagen.

- **Von diesen Benutzern/Gruppen kommend:** Wählen Sie diese Option, um Benutzer oder Benutzergruppen hinzufügen, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Tragen Sie die entsprechenden Benutzer oder Gruppen in das Feld *Benutzer/Gruppen* ein, das nach Auswahl der Bedingung geöffnet wird. Im Standardmodus funktioniert im Übrigen der Abgleich basierend auf bestimmten Benutzern/Gruppen nicht, weil die Authentifizierung entfällt.
- **Zu diesen Website-Kategorien gehend:** Wählen Sie diese Option, um Sicherheitsprüfungen für bestimmte Kategorien auszunehmen. Wählen Sie dann die Kategorien aus der Liste aus, die sich nach Auswahl der Bedingung öffnet.

3. **Klicken Sie auf *Speichern*.**
   Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

9.3.2 Websites

Auf der Registerkarte *Web Protection* > *Filteroptionen* > *Websites* können Sie Site-Listen verwalten, für die Sie die Standardkategorie oder den Ruf übergehen möchten.

So fügen Sie einen Eintrag zu *Lokale Site-Liste* hinzu:

1. **Klicken Sie auf die Schaltfläche *Site hinzufügen*.**
2. **Geben Sie die Sites für die Übergehung ein.**
   Im Textfeld im Dialogfeld *Lokale Site(s) hinzufügen* können URLs, Domänen, IP-Adressen oder CIDR-Bereiche eingegeben werden.
3. **Aktivieren Sie optional das Kontrollkästchen *Subdomänen einschließen*.**
   Wenn Sie dieses Kontrollkästchen aktivieren, werden die Übergehungen auf alle Subdomänen angewendet.Beispiel: Wenn Sie beispiel.de hinzufügen und das Kontrollkästchen *Subdomänen einschließen* aktivieren, wird auch mail.beispiel.de übergangen.
4. **Wählen Sie eine *Kategorie* oder einen *Ruf* aus, die/der übergangen werden soll.**
   Sie können entweder *Kategorie*, *Ruf* oder beides übergehen.Sites, die in *Lokale Site-Liste* definiert sind, werden durch Filteraktionen anhand dieser übergangenen Werte verarbeitet.
5. **Fügen Sie optional einen Kommentar hinzu.**

Bei großen Site-Listen können Sie mit den Symbolen *Weiter* und *Zurück* oben auf der Registerkarte durch die Einträge blättern oder mit dem Suchtextfeld nach Elementen suchen.Zum Löschen eines Eintrags klicken Sie auf das *Löschen*-Symbol neben dem betreffenden Eintrag. Oder wählen Sie mehrere Elemente aus und klicken Sie auf das *Löschen*-Symbol über der Liste.

9.3.3 Benutzer umgehen

Auf der Registerkarte *Web Protection > Filteroptionen > Benutzer umgehen* können Sie Benutzer oder Gruppen konfigurieren, die Blockierungen umgehen dürfen.

So fügen Sie eine vorhandene Gruppe oder einen vorhandenen Benutzer hinzu:

1. **Klicken Sie auf das Ordnersymbol neben *Benutzer/Gruppen, die Blockierungen umgehen dürfen*.**
   Die Liste der vorhandenen Benutzer und Gruppen wird im linken Navigationsbereich angezeigt.
2. **Wählen Sie den Benutzer oder die Gruppe aus und ziehen Sie ihn bzw. sie in das Feld *Benutzer/Gruppen, die Blockierungen umgehen dürfen*.**
   Das Element wird nun auf der Registerkarte *Benutzer umgehen* aufgeführt.

So fügen Sie einen neuen Benutzer hinzu:

1. **Klicken Sie auf das grüne Plussymbol neben *Benutzer/Gruppen, die Blockierungen umgehen dürfen*.**
   Das Dialogfeld *Benutzer hinzufügen* wird angezeigt.
2. **Geben Sie die Benutzerinformationen im Dialogfeld *Benutzer hinzufügen* ein**.
   Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.
3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

9.3.4 Potenziell unerwünschte Anwendungen

Auf der Registerkarte *Web Protection > Filteroptionen > PUAs* können Sie Listen autorisierter potenziell unerwünschter Anwendungen (PUAs) verwalten. Ihre UTM kann Anwendungen, die in einer Geschäftsumgebung potenziell unerwünscht sind, identifizieren und blockieren. Um bei aktiver Blockierung bestimmte PUAs zuzulassen, fügen Sie den Namen als gemeldet auf der Blockierungsseite oder in den Protokollen hinzu.

So fügen Sie einen Eintrag zu *Lokale Site-Liste* hinzu:

1. **Klicken Sie auf das *Plussymbol* in der Liste „Autorisierte PUA".**
2. **Geben Sie die PUA-Definition ein.**
   PUA-Definitionen finden Sie, indem Sie Protokolle & *Berichte > Web Protection > Internetnutzung* aufrufen und dann in der Auswahlliste *Verfügbare BerichtePUA-Downloads* auswählen.
3. **Klicken Sie auf *Übernehmen*.**

Klicken Sie auf das Menüsymbol *Aktionen öffnen* neben dem grünen *Plussymbol*, um eine Textliste von PUAs zu importieren oder exportieren und die Liste *Autorisierte PUA* zu löschen.

9.3.5 Kategorien

Auf der Registerkarte *Web Protection > Filteroptionen > Kategorien* können Sie die Zuordnung zwischen Website-Kategorien und Kategoriengruppen anpassen, die auf der Registerkarte *Filteraktion* oder auf der Seite *Websitefilter* ausgewählt werden können.Sophos UTM kann 60 unterschiedliche Kategorien von Websites identifizieren und den Zugriff auf sie blockieren. Ausgeklügelte URL-Klassifizierungsmethoden stellen die Genauigkeit und Vollständigkeit bei der Einschätzung fragwürdiger Websites sicher. Wenn ein Benutzer eine Webseite aufruft, die

nicht in der Datenbank vorliegt, wird die URL an Webcrawler gesendet und automatisch klassifiziert.

Hinweis – Wenn Sie der Meinung sind, dass eine Website falsch kategorisiert ist, können Sie dieses URL-Meldeformular verwenden, um neue Kategorien vorzuschlagen.

Um Website-Kategorien einer Kategoriengruppe zuzuordnen, gehen Sie folgendermaßen vor:

1. **Klicken Sie in der Kategoriengruppe, die Sie ändern wollen, auf *Bearbeiten*.**
   Das Dialogfeld *Filterkategorie bearbeiten* wird geöffnet.
2. **Wählen Sie die Unterkategorien aus.**
   Markieren Sie das Auswahlkästchen von Unterkategorien, die Sie hinzufügen wollen, oder entfernen Sie die Markierung von Unterkategorien, die Sie aus der Gruppe entfernen wollen.
3. **Klicken Sie auf *Speichern*.**
   Die Gruppe wird mit Ihren Einstellungen aktualisiert.

Alternativ können Sie auch eine neue Filterkategorie anlegen. Gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neue Filterkategorie* oben auf der Seite.**
   Das Dialogfeld *Filterkategorie erstellen* wird geöffnet.
2. **Geben Sie einen Namen ein.**
   Geben Sie einen aussagekräftigen Namen für die neue Filterkategorie ein.
3. **Wählen Sie die Unterkategorien aus.**
   Markieren Sie das Auswahlkästchen von Unterkategorien, die Sie zur Gruppe hinzufügen wollen.
4. **Klicken Sie auf *Speichern*.**
   Die Gruppe wird mit Ihren Einstellungen aktualisiert.

Um eine Kategorie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

9.3.6 HTTPS-CAs

Auf der Registerkarte *Web Protection* > *Webfilter* > *HTTPS-CAs* können Sie die Signierungs- und Verifizierungs-Zertifizierungsstellen (CAs) für HTTPS-Verbindungen verwalten.

Signierungs-CA

In diesem Abschnitt können Sie Ihr Signierungs-CA-Zertifikat hochladen, das Signierungs-CA-Zertifikat neu erstellen oder das vorhandene Signierungs-CA-Zertifikat herunterladen. Standardmäßig wird das Signierungs-CA-Zertifikat anhand der Informationen erstellt, die bei der Einrichtung angegeben wurden, d. h., dass sie den Informationen auf der Registerkarte *Verwaltung* > *Systemeinstellungen* > Organisatorisches entsprechen, sofern in der Zwischenzeit keine Änderungen vorgenommen wurden.

Um ein neues Signierungs-CA-Zertifikat hochzuladen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Hochladen*.**
   Das Dialogfenster *PKCS#12-Zertifikatsdatei hochladen* wird geöffnet.
2. **Navigieren Sie zu der Datei, die Sie hochladen wollen.**
   Klicken Sie auf das Ordnersymbol neben dem Feld *Datei*, klicken Sie im Dialogfenster *Datei hochladen* auf *Durchsuchen*, wählen Sie das hochzuladende Zertifikat aus und klicken Sie auf *Hochladen starten*.

   Sie können nur Zertifikate im PKCS#12-Format hochladen, die kennwortgeschützt sind.
3. **Geben Sie das Kennwort ein.**
   Geben Sie das Kennwort zweimal in die entsprechenden Felder ein und klicken Sie auf *Speichern*.

   Das neue Signierungs-CA-Zertifikat wird installiert.

Um Ihr Signierungs-CA-Zertifikat neu zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neu erstellen*.**
   Das Dialogfenster *Neue Signierungs-CA erstellen* wird geöffnet.
2. **Ändern Sie die Informationen.**
   Ändern Sie die angegebenen Informationen gemäß Ihren Bedürfnissen und klicken Sie auf *Speichern*.

   Das neue Signierungs-CA-Zertifikat wird erstellt. Die Informationen zur Signierungs-CA im Abschnitt *Signierungs-CA* ändern sich entsprechend.

Um das Signierungs-CA-Zertifikat herunterzuladen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Herunterladen*.**
   Das Dialogfenster *Zertifikatdatei herunterladen* wird geöffnet.

2. **Wählen Sie das Dateiformat aus, das Sie herunterladen wollen.**
   Sie können zwischen zwei verschiedenen Formaten wählen:
   - **PKCS#12:** Dieses Format ist verschlüsselt, geben Sie deshalb ein Kennwort für den Export ein.
   - **PEM:** Dieses Format ist unverschlüsselt.
3. **Klicken Sie auf *Herunterladen*.**
   Die Datei wird heruntergeladen.

Wenn Sie für Ihre internen Webserver Zertifikate verwenden, die von einer eigenen CA signiert sind, ist es ratsam, dieses CA-Zertifikat in den WebAdmin als vertrauenswürdige Zertifizierungsstelle (Trusted Certificate Authority) hochzuladen. Andernfalls wird Benutzern eine Fehlermeldung vom Webfilter angezeigt, die ihnen mitteilt, dass das Serverzertifikat nicht vertrauenswürdig ist.
Um die Ausstattung der Clients mit dem Proxy-CA-Zertifikat zu vereinfachen, können Benutzer das Zertifikat selbst über http://passthrough.fw-notify.net/cacert.pem herunterladen und es in ihrem Browser installieren. Die Website-Anfrage wird direkt vom Proxy akzeptiert und verarbeitet.Deshalb ist es notwendig, zunächst den Webfilter auf der Registerkarte *Webfilter > Allgemein* zu aktivieren.

Hinweis – Falls der Proxy nicht im *Transparenzmodus* arbeitet, muss der Proxy im Browser des Benutzers aktiviert werden. Sonst kann der Download-Link nicht erreicht werden.

Wenn das Benutzerportal aktiviert ist, können Benutzer alternativ das Proxy-CA-Zertifikat auch aus dem Benutzerportal, Registerkarte *HTTPS-Proxy*, herunterladen.

HTTPS-Problemen vorbeugen

Wenn Sie HTTPS verwenden, sind Windows-Systemprogramme wie Windows Update und Windows Defender nicht in der Lage, Verbindungen aufzubauen, weil sie mit `Systembenutzer`-Rechten laufen. Dieser Benutzer vertraut aber standardmäßig der Proxy-CA nicht. Deshalb ist es notwendig, das HTTPS-Proxy-CA-Zertifikat für den Systembenutzer zu importieren. Gehen Sie folgendermaßen vor:

1. **Öffnen Sie unter Windows die *Microsoft Management Console* (`mmc`).**
2. **Klicken Sie auf das Menü *Datei* und dann auf *Snap-In hinzufügen/entfernen*.**
   Das Dialogfenster *Snap-In hinzufügen/entfernen* wird geöffnet.

3. **Klicken Sie unten im Fenster auf *Hinzufügen*.**
   Das Dialogfenster *Eigenständiges Snap-In hinzufügen* wird geöffnet.
4. **Wählen Sie aus der Liste *Zertifikate* und klicken Sie auf *Hinzufügen*.**
   Ein Assistent wird geöffnet.
5. **Wählen Sie *Computerkonto* und klicken Sie auf *Weiter*.**
6. **Stellen Sie sicher, dass *Lokaler Computer* ausgewählt ist, und klicken Sie auf *Fertigstellen* und dann auf *Schließen*.**
   Das erste Dialogfenster enthält nun das Objekt *Zertifikate (Lokaler Computer)*.
7. **Klicken Sie auf *OK*.**
   Das Dialogfenster wird geschlossen und der Konsolenstamm enthält nun das Objekt *Zertifikate (Lokaler Computer)*.
8. **Öffnen Sie im *Konsolenstamm* links *Zertifikate* > *Vertrauenswürdige Stammzertifizierungsinstanzen*, klicken Sie mit der rechten Maustaste auf *Zertifikate* und wählen Sie *Alle Aufgaben* > *Importieren* aus dem Kontextmenü.**
   Der Import-Assistent wird geöffnet.
9. **Klicken Sie auf *Weiter*.**
   Der nächste Schritt wird angezeigt.
10. **Wechseln Sie zu dem zuvor heruntergeladenen HTTPS-Proxy-CA-Zertifikat, klicken Sie auf *Öffnen* und dann auf *Weiter*.**
    Der nächste Schritt wird angezeigt.
11. **Stellen Sie sicher, dass *Alle Zertifikate in folgendem Speicher speichern* ausgewählt ist, und klicken Sie dann auf *Weiter* und auf *Schließen*.**
    Der Import-Assistent meldet, dass der Import erfolgreich war.
12. **Bestätigen Sie die Meldung des Import-Assistenten.**
    Das Proxy-CA-Zertifikat wird nun unter den vertrauenswürdigen Zertifikaten aufgeführt.
13. **Speichern Sie die Änderungen.**
    Klicken Sie auf das Menü *Datei* und dann auf *Speichern*, um die Änderungen am Konsolenstamm zu speichern.

Nach diesem Importvorgang wird der CA systemweit vertraut und es sollten keine Verbindungsprobleme aufgrund des HTTPS-Proxys mehr auftreten.

Verifizierungs-CAs

In diesem Bereich können Sie Ihre Verifizierungs-CAs verwalten. Das sind Zertifizierungsstellen, denen Sie generell vertrauen, d. h. Websites, die gültige Zertifikate

vorweisen, welche von diesen CAs signiert sind, werden vom HTTPS-Proxy als vertrauenswürdig eingestuft.

Lokale Verifizierungs-CAs: Sie können weitere Verifizierungs-CAs zur untenstehenden CA-Liste hinzufügen. Gehen Sie folgendermaßen vor:

1. **Klicken Sie auf das Ordnersymbol neben dem Feld *Lokale CA hochladen*.**
   Das Dialogfeld *Datei hochladen* öffnet sich.

2. **Wählen Sie das Zertifikat aus, das Sie hochladen wollen.**
   Klicken Sie auf *Durchsuchen* und wählen Sie das CA-Zertifikat aus, das Sie hochladen wollen. Nur PEM-Dateierweiterungen werden für Zertifikate unterstützt:

3. **Laden Sie das Zertifikat hoch.**
   Klicken Sie auf *Hochladen starten*, um das gewählte Zertifikat hochzuladen.

   Das Zertifikat wird installiert und im Abschnitt *Lokale Verifizierungs-CAs* angezeigt.

Globale Verifizierungs-CAs: Die Liste der hier aufgeführten Verifizierungs-CAs ist identisch mit den Verifizierungs-CAs, die in Mozilla Firefox vorinstalliert sind. Sie können jedoch einen oder alle Verifizierungs-CAs auf der Liste deaktivieren, wenn Sie sie nicht für vertrauenswürdig halten. Um das Zertifikat zurückzuziehen (engl. revoke), klicken Sie auf seinen Schieberegler. Der Schieberegler wird daraufhin grau und der HTTP-Proxy akzeptiert nun keine Websites mehr, die von dieser CA signiert sind.

Tipp – Klicken Sie auf das blaue Infosymbol, um den Fingerabdruck der CA zu sehen.

Der HTTPS-Proxy zeigt Clients eine Fehlerseite mit dem Hinweis „Blocked Content“, wenn die CA unbekannt oder deaktiviert ist.Sie können jedoch eine Ausnahme für solche Seiten erstellen: entweder über den Link *Ausnahme anlegen* auf der Fehlerseite des Webfilters oder über die Registerkarte *Web Protection* > *Webfilter* > *Ausnahmen*.

Hinweis – Wenn Sie auf den Link *Ausnahme anlegen* auf der Fehlerseite des Webfilters klicken, wird ein Anmeldedialog angezeigt.Nur Benutzer mit Admin-Rechten können Ausnahmen anlegen.

9.3.7 Sonstiges

Die Registerkarte *Web Protection* > *Filteroptionen* > *Sonstiges* bietet zusätzliche Konfigurationsoptionen für den Webfilter, z. B. Zwischenspeicherung (Caching), Streaming oder Porteinstellungen.

Sonstige Einstellungen

Webfilter-Port: In diesem Eingabefeld wird die Portnummer für Client-Anfragen an den Webfilter festgelegt.Standardmäßig ist der Port `8080` eingetragen.

> **Hinweis –** Die Option ist nur gültig, wenn der Proxy nicht im Transparenzmodus arbeitet.

MIME-Blockierung untersucht HTTP-Body: Nicht nur der HTTP-Header wird auf blockierte MIME-Typen überprüft, sondern auch der HTTP-Body. Beachten Sie, dass das Einschalten dieser Funktion sich negativ auf die Leistung des Systems auswirken kann.

Unscannbare und verschlüsselte Dateien blockieren: Wählen Sie diese Option, um Dateien zu blockieren, die nicht gescannt werden konnten. Der Grund hierfür kann unter anderem sein, dass Dateien verschlüsselt oder beschädigt sind.

Zugelassene Zieldienste: Wählen Sie aus dem Feld *Zugelassene Zieldienste* die Dienste aus, auf die der Webfilter zugreifen darf. Standardmäßig sind bereits die Dienste mit Ports enthalten, zu denen eine Verbindung als sicher gilt und die in der Regel von Browsern genutzt werden: *HTTP* (Port `80`), *HTTPS* (Port `443`), *FTP* (Port `21`), *LDAP* (Port `389`), *LDAP-SSL* (Port `636`), *Webfilter* (Port `8080`), *UTM Spam Release* (Ports `3840–4840`) und *UTM WebAdmin* (Port `4444`).

Standardzeichensatz: Diese Option wirkt sich darauf aus, wie der Proxy Dateinamen im Fenster *Download-Verwaltung* anzeigt. URLs (und Dateinamen, auf die sie vielleicht verweisen), die in ausländischen Zeichensätzen codiert sind, werden von UTF-8 in den hier definierten Zeichensatz umgewandelt, es sei denn, der Server übermittelt einen anderen Zeichensatz. Wenn Sie sich in einem Land oder einer Region befinden, die einen Zwei-Byte-Zeichensatz verwendet, sollten Sie diese Option auf den „nativen“ Zeichensatz für dieses Land/diese Region setzen.

Suchdomäne: Sie können hier eine zusätzliche Domäne angeben, die durchsucht wird, wenn der erste DNS-Lookup kein Ergebnis liefert („NXDOMAIN“). Dann wird eine zweite DNS-Anfrage gestartet, die die hier angegebene Domäne an den ursprünglichen Hostnamen anhängt. Beispiel: Ein Benutzer gibt `http://wiki` ein und meint damit *wiki.intranet.beispiel.de*. Die URL kann jedoch nur aufgelöst werden, wenn Sie `intranet.beispiel.de` in das Feld *Suchdomäne* eintragen.

Authentifizierungs-Zeitüberschreitung: Mit dieser Einstellung können Sie festlegen, wie lange (in Sekunden) ein Benutzer nach dem Anmelden mit der Authentifizierung im Browsermodus browsen kann. Wenn der Benutzer eine Abmelderegisterkarte geöffnet hat, kann er

weiter browsen, ohne sich neu authentifizieren zu müssen, bis diese Registerkarte geschlossen wird, zuzüglich Authentifizierungs-Zeitüberschreitung.

Mit dieser Einstellung können Sie zudem einstellen, wie lange (in Sekunden) eine *Blockierungsumgehung* oder ein *Fortfahren bei Warnung* dauert.

Authentifizierungsbereich: Der Authentifizierungsbereich (engl. authentication realm) ist der Name der Quelle, die ein Browser zusammen mit der Authentifzierungsanfrage anzeigt, wenn der Proxy im Modus *Einfache Benutzerauthentifizierung* arbeitet. Er legt den geschützten Bereich entsprechend der Spezifikation RFC 2617 fest. Sie können hier einen beliebigen Ausdruck eingeben.

Transparenzmodus-Ausnahmen

Diese Option ist nur von Bedeutung, wenn der Webfilter im Transparenzmodus arbeitet. Hosts und Netzwerke, die in den Feldern *Hosts/Netze vom Transparenzmodus ausnehmen* aufgeführt sind, werden vom HTTP-Proxy nicht transparent überwacht. Es gibt ein Feld für Quell- und eins für Zielhosts/-netzwerke. Um dennoch HTTP-Datenverkehr (ohne Proxy) für alle diese Hosts und Netzwerke zu erlauben, wählen Sie die Option *HTTP-Verkehr für aufgeführte Hosts/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezielle Firewallregeln für die hier aufgeführten Hosts und Netzwerke anlegen.

Automatische Proxy-Konfiguration (Proxy Auto Configuration)

Die automatische Proxy-Konfiguration ist eine Funktion, die es Ihnen ermöglicht, eine automatische Proxy-Konfigurationsdatei (PAC-Datei, Proxy Auto Configuration) zentral bereitzustellen, welche dann von Browsern selbsttätig abgeholt werden kann. Die Browser wiederum konfigurieren ihre Proxy-Einstellungen nach den Angaben, die in der PAC-Datei aufgeführt sind.

Die PAC-Datei heißt *wpad.dat*, hat den MIME-Typ `application/x-ns-proxy-autoconfig` und wird von der UTM bereitgestellt. Sie enthält die Informationen, die Sie in das Textfeld eingeben, z.B.:

```
function FindProxyForURL(url, host)
 { return "PROXY proxy.example.com:8080; DIRECT"; }
```

Die obige Funktion weist den Browser an, alle Seitenanfragen an den Proxy-Server `proxy.beispiel.de` auf Port `8080` umzuleiten. Wenn der Proxy nicht erreichbar ist, wird eine direkte Verbindung mit dem Internet hergestellt.

Der Hostname kann auch als Variable `${asg_hostname}`. Das ist sehr nützlich, wenn Sie mit dem UTM Manager die selbe PAC-Datei auf mehreren Sophos UTM-Appliances anwenden

möchten. Die Variable wird dann mit dem Hostnamen der jeweiligen UTM umschrieben. Mit der Varibale im oberen Beispiel, würde das dann wie folgt aussehen:

```
function FindProxyForURL(url, host)
 { return "PROXY ${asg_hostname}:8080; DIRECT"; }
```

Um eine PAC-Datei für Ihr Netzwerk bereitzustellen, haben Sie die folgenden Möglichkeiten:

- Bereitstellung über Browserkonfiguration: Wenn Sie die Option *Automatische Proxy-Konfiguration aktivieren* auswählen, steht die PAC-Datei unter folgender URL über den UTM-Webfilter zur Verfügung: `http://IP-of-UTM:8080/wpad.dat`. Um diese Datei zu verwenden, geben Sie ihre URL in der automatischen Proxy-Konfigurationseinstellung jener Browser an, die den Proxy verwenden sollen.
- Bereitstellung über DHCP: Sie können dafür sorgen, dass Ihr DHCP-Server die URL der PAC-Datei zusammen mit der Client-IP-Adresse vergibt. Wählen Sie dazu die Option *Automatische Proxy-Konfiguration aktivieren* in Ihrer DHCP-Serverkonfiguration aus (siehe Kapitel *Netzwerkdienste* > *DHCP*). Ein Browser holt sich dann automatisch die PAC-Datei ab und konfiguriert seine Einstellungen entsprechend.

> **Hinweis –** Die Bereitstellung über DHCP funktioniert ausschließlich mit dem Microsoft Internet Explorer. Bei allen anderen Browsern müssen Sie die PAC-Datei manuell bereitstellen.

Übergeordneter Proxy für URL-Kategorisierung

Geben Sie einen Proxy-Server für die URL-Kategorisierungssuche ein, wenn Sie keinen direkten Internetzugriff haben. Diese Option ist nur verfügbar, wenn bei Ihnen Endpoint Protection aktiviert ist oder wenn Sie lokale Suchanfragen durchführen. Bei lokalen Suchanfragen legen Sie mit dieser Option den Proxy fest, der zum Herunterladen von Kategorisierungsaktualisierungen in die UTM verwendet wird.

Webfilter-Zwischenspeicherung

Zwischenspeichern aktivieren: Wenn diese Option aktiviert ist, hält der Webfilter einen Zwischenspeicher auf Festplatte vor, um Anfragen zu häufig besuchten Webseiten schneller beantworten zu können.

- **SSL-Inhalte zwischenspeichern:** Wählen Sie diese Option, um SSL-verschlüsselte Daten ebenfalls – unverschlüsselt – auf der Festplatte zu speichern.
- **Inhalte mit Cookies zwischenspeichern:** Cookies werden oft für Authentifizierungszwecke verwendet. Wenn diese Option aktiviert ist, werden HTTP-Antworten,

die Cookies enthalten, ebenfalls zwischengespeichert. Dieses Vorgehen kann aber zu Datenschutz-Problemen führen, da Benutzer, die auf die gleiche Seite zugreifen wollen, sehr wahrscheinlich die Seite aus dem Cache erhalten, welche dann den Cookie eines anderen Benutzers enthält.

> **Wichtiger Hinweis –** Das Zwischenspeichern von SSL- und/oder Cookie-Inhalten stellt ein wichtiges Sicherheitsproblem dar, da die Inhalte von jedem Benutzer mit SuperAdmin-Rechten eingesehen werden können.

- **Zwischenspeichern für Sophos-Endpoint-Aktualisierungen erzwingen:** Wenn die Option aktiviert ist, werden bestimmte Daten, die im Zusammenhang mit Endpoint-Anfragen an Sophos-Auto-Update (SAU) stehen, zwischengespeichert. Wir empfehlen, diese Funktion zu aktivieren, wenn Sie Endpoint Protection verwenden. Ist die Option deaktiviert, werden diese Daten nicht zwischengespeichert. Dies kann zu Uplink-Engpässen führen, wenn viele Endpoints gleichzeitig versuchen, Daten von den Update-Servern im Internet herunterzuladen.

Zwischenspeicher leeren: Sie können alle zwischengespeicherten Seiten löschen, indem Sie auf *Zwischenspeicher leeren* klicken.

Streaming-Einstellungen

Streaming-Inhalte nicht scannen: Wenn diese Option aktiviert ist, werden typische Audio- und Video-Streaming-Inhalte nicht auf ihren Inhalt hin gescannt. Das Abschalten dieser Option wird die meisten Mediastreams praktisch deaktivieren, da sie nicht in vertretbarer Zeit gescannt werden können. Daher wird empfohlen, diese Option eingeschaltet zu lassen.

Apple OpenDirectory Single Sign-On

Wenn Sie *Apple OpenDirectory SSO* als Authentifizierungsmethode nutzen, müssen Sie eine MAC OS X Single Sign-On Kerberos-Schlüsseldatei hochladen, damit die Authentifizierung funktioniert. Generieren Sie die Schlüsseldatei und laden Sie sie durch einen Klick auf das Ordnersymbol hoch. Weitere Informationen dazu, wie Sie die Schlüsseldatei generieren können, finden Sie in der Kerberos-Dokumentation.

Zertifikat für Endbenutzerseiten

Die UTM verwendet HTTPS für Benutzerbenachrichtigungen, zur Browserauthentifizierung und anderen sicheren Benutzerinteraktionen. Standardmäßig verwendet die UTM ein automatisch generiertes Zertifikat für diese HTTPS-Verbindungen. Sie können mit dieser Option ein benutzerdefiniertes Zertifikat für HTTPS-Seiten verwenden, die dem Endbenutzer

angezeigt werden. Um ein eigenes, benutzerdefiniertes Zertifikat für diese HTTPS-Verbindungen zu verwenden, laden Sie es zunächst über *Fernzugriff > Zertifikatverwaltung > Zertifikate* hoch und wählen Sie es dann aus und aktualisieren Sie Ihre Einstellungen hier.

Hinweis –Der angegebene *Hostname:* ist die Basisdomäne für das Zertifikat, das Sie verwenden.Die UTM hängt dann das Präfix *passthrough.*oder *passthrough6.* für diese Domäne an. Das Zertifikat muss für *passthrough* (und *passthough6*) als Common Name, Subject Alternate Name oder, was am häufigsten vorkommt, als Platzhalterzertifikat gültig sein, sodass Sie jeden Host als Präfix an die Domäne anhängen können.Außerdem müssen Sie als DNS für *passthrough* und *passthrough6* bestimmte IP-Adressen einstellen. Wenn Sie die UTM als DNS-Server verwenden, erfolgt dies automatisch. Wenn Sie einen anderen DNS-Server verwenden, müssen Sie diese Einträge dort erstellen.

9.4 Richtlinientest

Auf der Seite *Web Protection > Richtlinientest* können Sie URLs mit Ihren vorhandenen *Webfilter-Profilen* testen. Um eine URL mit Ihrer aktuellen Richtlinie zu testen, gehen Sie wie folgt vor:

1. **Geben Sie die URL ein, die Sie testen möchten.**
2. **Geben Sie die Quell-IP-Adresse ein.**
   Unterschiedliche Quellnetzwerke weisen möglicherweise unterschiedliche *Webfilter-Profile* auf.
3. **Geben Sie optional einen Benutzer ein, unter dessen Identität Sie die Anfrage testen möchten.**
   Benutzer können unter unterschiedliche *Webfilter-Profile* fallen.
4. **Geben Sie optional einen Zeitpunkt für die Anfrage ein.**
   Webfilter-Profile können mit tageszeitbasierten Regeln konfiguriert werden.
5. **Klicken Sie auf „Test“.**

Die Ergebnisse Ihrer Testparameter werden im Feld *Richtlinientestergebnisse* angezeigt.

Hinweis – Wenn Sie eine URL mir Ihren *Webfilter-Profilen* testen, lädt die Seite *Web Protection > Richtlinientest* keine Inhalte herunter und führt keine Überprüfungen auf Schad-

software, MIME-Typen oder Dateierweiterungen durch. Das tatsächliche Filterverhalten kann je nach den von der URL gehosteten Inhalten abweichen.

Hinweis – Der korrekte Authentifizierungsserver muss auf der Seite *Definitionen & Benutzer > Authentifizierungsdienste > Server* hinzugefügt werden, damit der Test funktioniert.

9.5 Application Control

Die Application-Control-Funktion von UTM ermöglicht Ihnen Traffic Shaping und Blockieren von Netzwerkverkehr basierend auf der Art des Verkehrs. Im Gegensatz zur Webfilter-Funktion von UTM (siehe Kapitel Webfilter) unterscheidet der Klassifizierungsmechanismus von Application Control Netzwerkverkehr nicht nur nach Protokoll oder URL, sondern nimmt detailliertere Unterscheidungen vor. Besonders bei Internetverkehr ist dies nützlich: Verkehr zu Websites erfolgt normalerweise über das HTTP-Protokoll auf Port 80 oder das HTTPS-Protokoll auf Port 443. Wenn Sie Verkehr zu einer bestimmten Website, z. B. facebook.com, blockieren möchten, können Sie das auf Grundlage der URL der Website (Webfilter) konfigurieren. Sie können Verkehr zu Facebook auch unabhängig von einer URL über eine Klassifizierung des Netzwerkverkehrs blockieren.

Die Klassifizierungsengine von UTM nutzt Layer-7-Packet-Inspection für die Klassifizierung von Netzwerkverkehr.

Application Control kann auf zweifache Weise genutzt werden. In einem ersten Schritt müssen Sie Application Control auf der Seite *Netzwerksichtbarkeit* generell aktivieren, sodass Anwendungen in gewisser Hinsicht „sichtbar" werden. Jetzt können Sie die Einstellung so bestehen lassen (beispielsweise für einen bestimmten Zeitraum), um zu sehen, welche Anwendungen von den Benutzern genutzt werden (z. B. im Flow-Monitor, in der Protokollierung, in der Berichterstellung). In einem zweiten Schritt können Sie bestimmte Anwendungen blockieren und andere zulassen. Dies erreichen Sie mit Hilfe von Regeln, die auf der Seite *Application-Control-Regeln* erstellt werden können. Zudem können Sie festlegen, dass Datenverkehr bestimmter Anwendungen bevorzugt behandelt wird. Die Konfiguration erfolgt über die Dienstqualität-Funktion (QoS) von Sophos.

9.5.1 Netzwerksichtbarkeit

Auf der Seite *Web Protection* > *Application Control* > *Netzwerksichtbarkeit* können Sie Application Control aktivieren und deaktivieren.

Wenn Application Control aktiviert ist, wird der gesamte Netzwerkverkehr klassifiziert und entsprechend seiner Klassifizierung protokolliert. Aktueller Netzwerkverkehr kann über den Flow-Monitor mit detaillierten Angaben zur Art des Datenverkehrs angezeigt werden (siehe Kapitel *Flow-Monitor*). So werden beispielsweise Daten zum HTTP-Verkehr detailliert aufgeschlüsselt, sodass die zugrunde liegenden Anwendungen (z. B. Twitter, Facebook usw.) ersichtlich sind. Um den Flow-Monitor zu öffnen, wählen Sie die gewünschte Schnittstelle im Bereich *Flow-Monitor* und klicken Sie auf *Flow-Monitor öffnen*.

Für Protokollierung und Berichterstellung sind umfangreiche Daten zu Netzwerkverkehr und Klassifizierung sowie Daten zu Clients und Servern verfügbar, die die Anwendungen nutzen.Weitere Informationen zu Protokollierung und Berichterstellung finden Sie im Kapitel *Protokollierung & Berichterstellung*. Lesen Sie den Abschnitt *Protokolldatei-Ansicht* für die Protokollierung und den Abschnitt *Netzwerknutzung* > *Bandbreitennutzung* und *Web Protection* > *Application Control* für die Berichterstellung.

9.5.2 Application-Control-Regeln

Auf der Seite *Web Protection* > *Application Control* > *Application-Control-Regeln* können Sie Regeln erstellen, die auf einer Klassifizierung des Netzwerkverkehrs basieren und Anwendungen definieren, deren Datenverkehr für Ihr Netzwerk blockiert oder ausdrücklich zugelassen werden soll.

Standardmäßig wird sämtlicher Netzwerkverkehr zugelassen, wenn Application Control aktiviert ist.

Application-Control-Regeln können entweder auf dieser Seite oder über den Flow-Monitor erstellt werden. Letzteres ist eventuell bequemer, doch so können Sie nur Regeln für den aktuell im Netzwerk auftretenden Datenverkehr erstellen.

Um eine Application-Control-Regel zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Application-Control-Regeln* auf *Neue Regel*.**
   Das Dialogfeld *Neue Regel anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

   Name (optional): Sie können einen Namen für die Regel eingeben. Wenn Sie das Feld leer lassen, generiert das System einen Namen für die Regel.

   Gruppe: Die Option *Gruppe* dient dazu, Regeln logisch zusammenzufassen. Mit der Auswahlliste über der Liste können Sie die Regeln nach ihrer Gruppe filtern. Die Zugehörigkeit zu einer Gruppe hat nur Auswirkungen auf die Darstellung, aber keinen Einfluss auf die Abarbeitung der Regeln. Um eine Gruppe anzulegen, wählen Sie den Eintrag << *Neue Gruppe* >> und geben Sie einen aussagekräftigen Namen in das Feld *Name* ein.

   Position: Die Positionsnummer legt die Priorität der Regel fest. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Sobald eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen.

   Aktion: Wählen Sie aus, ob der Datenverkehr blockiert oder zugelassen werden soll.

   Kontrollieren durch: Wählen Sie aus, ob der Datenverkehr nach Anwendungsart oder durch einen dynamischen Filter kontrolliert werden soll, der unterschiedliche Kategorien berücksichtigt.

   - **Anwendungen:** Der Datenverkehr wird anwendungsbasiert kontrolliert. Wählen Sie im Feld *Diese Anwendungen kontrollieren* eine oder mehrere Anwendungen aus.

   - **Dynamischer Filter:** Der Datenverkehr wird basierend auf Kategorien kontrolliert. Wählen Sie im Feld *Diese Kategorien kontrollieren* eine oder mehrere Kategorien aus.

   Diese Anwendungen/Kategorien kontrollieren: Klicken Sie auf das Ordnersymbol, um Anwendungen/Kategorien auszuwählen. Ein Dialogfenster wird geöffnet, das im nächsten Abschnitt detailliert beschrieben wird.

   Hinweis – Einige Anwendungen können nicht blockiert werden. Dies ist für einen reibungslosen Betrieb von Sophos UTM erforderlich. Bei diesen Anwendungen wird in der Anwendungstabelle des Dialogfensters *Anwendung auswählen* kein Auswahlkästchen angezeigt. Dies trifft u. a. für den *WebAdmin*, *Teredo*, *SixXs* (für IPv6-Verkehr) und *Portal* (für Benutzerportal-Verkehr) zu. Auch bei der Verwendung dynamischer Filter wird das Blockieren dieser Anwendungen automatisch verhindert.

Produktivität (nur mit *Dynamischer Filter*): Gibt den von Ihnen gewählten Produktivitätswert wieder.

Risiko (nur mit *Dynamischer Filter*): Gibt den von Ihnen gewählten Risikowert wieder.

Für: Wählen Sie in diesem Feld Netzwerke oder Hosts aus, deren Netzwerkverkehr von der Regel kontrolliert werden soll. Sie können auch Netzwerke oder Hosts hinzufügen. Dies gilt nur für Quellhosts/-netzwerke.Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Protokollieren: Diese Option ist standardmäßig ausgewählt und ermöglicht das Protokollieren von Datenverkehr, auf den die Regel zutrifft.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Regel wird in der Liste *Application-Control-Regeln* angezeigt.

Das Dialogfenster zur Auswahl von Anwendungen oder Kategorien

Beim Erstellen von Application-Control-Regeln müssen Sie Anwendungen oder Anwendungskategorien aus dem Dialogfenster *Wählen Sie eine oder mehrere Anwendungen/Kategorien, die kontrolliert werden sollen* festlegen.

In der Tabelle im unteren Bereich des Dialogfensters werden die Anwendungen angezeigt, die auswählbar sind oder zu einer definierten Kategorie gehören. Standardmäßig werden alle Anwendungen angezeigt.

Im oberen Bereich des Dialogfensters stehen drei Konfigurationsoptionen zur Wahl, mit deren Hilfe die Anzahl der in der Tabelle gelisteten Anwendungen eingeschränkt werden kann:

- **Kategorie:** Die Anwendungen werden nach Kategorie gruppiert. Diese Liste umfasst alle verfügbaren Kategorien. Standardmäßig sind alle Kategorien ausgewählt; d. h. alle verfügbaren Anwendungen werden unten in der Tabelle gelistet. Möchten Sie die angezeigten Anwendungen auf bestimmte Kategorien beschränken, klicken Sie in die Liste mit den Kategorien und wählen Sie nur die gewünschte(n) Kategorie(n) aus.

- **Produktivität:** Die Anwendungen werden zudem nach ihrer Auswirkung auf die Produktivität klassifiziert, d. h., wie stark sie die Produktivität beeinflussen. Beispiel: Salesforce, eine typische Unternehmenssoftware, besitzt die Bewertung 5. Die Nutzung der Anwendung trägt somit zur Produktivität bei. Im Gegensatz dazu ist das Onlinespiel Farm-

ville mit 1 bewertet und dadurch kontraproduktiv. Der Netzwerkdienst DNS besitzt die Bewertung 3 – er wirkt sich neutral auf die Produktivität aus.

- **Risiko:** Anwendungen werden auch hinsichtlich ihres Risikos bezüglich Schadsoftware, Virusinfektionen oder Angriffen klassifiziert. Je höher die Bewertung, desto höher das Risiko.

Tipp – Jede Anwendung verfügt über ein Infosymbol. Wenn Sie darauf klicken, wird eine Beschreibung der jeweiligen Anwendung angezeigt. Sie können die Tabelle mit Hilfe des Filterfelds in der Kopfzeile durchsuchen.

Abhängig davon, welchen Kontrolltyp Sie im Dialogfeld *Neue Regel anlegen* ausgewählt haben, gehen Sie folgendermaßen vor:

- Kontrolle durch dynamischen Filter: Wählen Sie im Feld *Kategorie* die Kategorien aus und klicken Sie auf *Übernehmen*, um die ausgewählten Kategorien für die Regel zu übernehmen.
- Anwendungsbasierte Kontrolle: Wählen Sie die zu kontrollierenden Anwendungen in der Tabelle aus, indem Sie auf die Auswahlkästchen klicken, die vor den Anwendungen angezeigt werden. Klicken Sie auf *Übernehmen*, um die ausgewählten Anwendungen für die Regel zu übernehmen.

Nachdem Sie auf *Übernehmen* geklickt haben, wird das Dialogfenster geschlossen und Sie können die Einstellungen der Anwendungsregel weiter bearbeiten.

9.5.3 Erweitert

Auf der Seite *Web Protection* > *Application Control* > *Erweitert* können Sie erweiterte Optionen für Application Control konfigurieren.

Application-Control-Ausnahmen

In diesem Feld aufgeführte Hosts und Netzwerke werden nicht von Application Control überwacht und können deshalb weder von Application Control noch von der Quality-of-Service-Auswahl kontrolliert werden. Das gilt sowohl für Quell- als auch für Zielhosts/-netzwerke.

9.6 FTP

Auf der Registerkarte *Web Protection > FTP* können Sie den FTP-Proxy konfigurieren. Das *File Transfer Protocol* (FTP) ist ein weit verbreitetes Netzwerkprotokoll, um Dateien über das Internet auszutauschen. Sophos UTM bietet einen Proxydienst, der als Zwischenstation für allen FTP-Verkehr in Ihrem Netzwerk agiert. Dabei bietet der FTP-Proxy nützliche Funktionen wie das Scannen von FTP-Verkehr auf Viren oder das Blockieren von bestimmten Dateitypen, die über das FTP-Protokoll übertragen werden.

Der FTP-Proxy kann transparent arbeiten, das heißt, alle FTP-Clients in Ihrem Netzwerk bauen eine Verbindung mit dem Proxy auf anstatt mit dem wirklichen Zielhost. Der Proxy initiiert dann anhand der Anfrage eine neue Netzwerkverbindung, die für den Client unsichtbar bleibt. Der Vorteil dieses Modus ist, dass keine zusätzliche Verwaltung oder Client-seitige Konfiguration nötig ist.

9.6.1 Allgemein

Auf der Registerkarte *Web Protection > FTP > Allgemein* können Sie die Grundeinstellungen für den FTP-Proxy vornehmen.

Um den FTP-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den FTP-Proxy auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *FTP-Einstellungen* kann bearbeitet werden.

2. **Wählen Sie die zugelassenen Netzwerke aus.**
   Wählen Sie die Netzwerke aus, die den FTP-Proxy verwenden dürfen.

3. **Wählen Sie einen Betriebsmodus aus.**
   Wählen Sie einen Betriebsmodus für den FTP-Proxy aus. Die folgenden Modi sind möglich:

   - **Transparent:** Der Proxy leitet die Client-Anfragen an den Zielserver weiter und scannt den Inhalt. Es ist keine Konfiguration auf Client-Seite notwendig.

   - **Nicht transparent:** Für diesen Modus müssen Sie die FTP-Clients konfigurieren. Verwenden Sie die IP-Adresse des Gateways und Port `2121`.

- **Beide:** Dieser Modus ermöglicht Ihnen, für einige Clients den transparenten Modus zu verwenden und für andere den nicht transparenten Modus. Konfigurieren Sie für die FTP-Clients, die im nicht transparenten Modus betrieben werden sollen, die Verwendung eines Proxy mit der IP-Adresse des Gateways und Port `2121`.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Hinweis – Der FTP-Proxy kann nicht mit FTP-Servern kommunizieren, die Active Directory als Authentifizierungsmethode verwenden. Um FTP-Clients zu ermöglichen, sich mit einem solchen FTP-Server zu verbinden, fügen Sie den FTP-Server zu den FTP-Proxy-Ausnahmen auf der Registerkarte *Erweitert* hinzu.

9.6.2 Antivirus

Die Registerkarte *Web Protection* > *FTP* > *Antivirus* bietet alle Maßnahmen gegen FTP-Verkehr, der schädliche und gefährliche Inhalte wie Viren, Würmer und andere Malware verbreitet.

Antiviren-Scan verwenden: Wenn Sie diese Option wählen, wird der gesamte eingehende FTP-Datenverkehr gescannt. Sophos UTMbietet mehrere Antiviren-Mechanismen für höchste Sicherheit.

- **Einzelscan:** Standardeinstellung; bietet maximale Leistung. Die auf der Registerkarte *Systemeinstellungen* > *Scan-Einstellungen* festgelegte Engine wird verwendet.
- **Zweifachscan:** Bietet maximale Erkennungsrate, da der entsprechende Verkehr von zwei verschiedenen Virenscannern gescannt wird. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist.

Max. Scangröße: Legen Sie die Maximalgröße von Dateien fest, die von den Antiviren-Engines gescannt werden sollen. Dateien, die größer sind, werden nicht gescannt.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – In Archiven (z. B. `zip`-Dateien) gespeicherte Dateien können nicht nach blockierten Dateitypen, blockierten Erweiterungen oder blockierten MIME-Typen durchsucht werden. Wenn Sie Ihr Netzwerk vor diesen in Archiven gespeicherten Dateien schützen möchten, sollten Sie Dateitypen wie zip, rar usw. generell blockieren.

Dateierweiterungenfilter

Diese Funktion filtert bestimmte FTP-Transfers basierend auf den übermittelten Dateierweiterungen (z. B. ausführbare Binärdateien) aus dem Internetverkehr heraus, wenn diese eine Dateierweiterung besitzen, die in der Liste *Blockierte Erweiterungen* aufgeführt ist. Sie können weitere Dateierweiterungen hinzufügen oder solche Erweiterungen aus der Liste löschen, die nicht blockiert werden sollen. Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Blockierte Erweiterungen* und geben Sie die Dateierweiterung ein, die blockiert werden soll, zum Beispiel `exe` (ohne den Punkt als Trennzeichen). Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

9.6.3 Ausnahmen

Auf der Registerkarte *FTP > Ausnahmen* können Sie Hosts/Netzwerke definieren, die von bestimmten Sicherheitsoptionen, die der FTP-Proxy bietet, ausgenommen werden sollen.

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahmenliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Ausnahme ein.

   Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, die nicht durchgeführt werden sollen:

   - **Antivirenprüfung:** Wählen Sie diese Option, um die Virenscanfunktion zu deaktivieren, die Datenverkehr nach unerwünschten Inhalten wie Viren, Trojanischen Pferden und Ähnlichem durchsucht.

   - **Blockierung von Dateierweiterungen:** Wählen Sie diese Option, um den Dateierweiterungenfilter zu deaktivieren, der verwendet werden kann, um Dateiübertragungen basierend auf Dateierweiterungen zu blockieren.

   - **Zugelassene Server:** Wählen Sie diese Option, um Prüfungen für zugelassene Server zu deaktivieren, die auf der Registerkarte *Erweitert* angegeben werden können. Wenn diese Option ausgewählt ist, können die gewählten Clienthosts/-netzwerke auf alle FTP-Server zugreifen und die gewählten Serverhosts/-netzwerke sind für alle Clients erlaubt.

Für diese Clienthosts/-Netzwerke: Wenn Sie diese Option wählen, wird das Feld *Clienthosts/-netzwerke* geöffnet. Wählen Sie die Clienthosts/-netzwerke aus, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen.

ODER Für diese Serverhosts/-Netzwerke: Wenn Sie diese Option wählen, wird das Feld *Serverhosts/-netzwerke* geöffnet. Wählen Sie die Serverhosts/-netzwerke aus, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

9.6.4 Erweitert

Auf der Registerkarte *FTP > Erweitert* können Sie Hosts und Netzwerke angeben, die nicht mit dem Transparenzmodus des FTP-Proxys überwacht werden sollen. Außerdem können Sie festlegen, auf welche FTP-Server zugegriffen werden darf.

FTP-Proxy-Ausnahmen

Hier aufgeführte Hosts und Netzwerke (sowohl FTP-Clients als auch FTP-Server) sind von der transparenten Überwachung des FTP-Verkehrs ausgenommen. Um jedoch FTP-Verkehr für diese Hosts und Netzwerke zuzulassen, wählen Sie die Option *FTP-Verkehr für aufgeführte Hosts/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezielle Firewallregeln für die hier aufgeführten Hosts und Netzwerke anlegen.

Hinweis – Der FTP-Proxy kann nicht mit FTP-Servern kommunizieren, die Active Directory als Authentifizierungsmethode verwenden. Damit sich FTP-Clients mit einem solchen FTP-Server verbinden können, fügen Sie den Server zu den FTP-Proxy-Ausnahmen hinzu.

FTP-Server

Wählen Sie FTP-Server aus oder fügen Sie FTP-Server hinzu, auf die von Ihren Hosts/Ihrem Netzwerk aus zugegriffen werden darf. Sie können Ausnahmen für einige FTP-Clients oder FTP-Server auf der Registerkarte *Ausnahmen* anlegen, um diese Liste zu umgehen.

10 Email Protection

In diesem Kapitel wird beschrieben, wie Sie die grundlegenden Email-Protection-Funktionen von Sophos UTM konfigurieren. Die Seite *Email-Protection-Statistik* in WebAdmin liefert einen Überblick über die zehn aktivsten E-Mail-Versender, E-Mail-Empfänger, Spam-Versender (nach Land), erkannte Schadsoftware und gleichzeitige Verbindungen des aktuellen Datums.In jedem Abschnitt befindet sich ein Link auf die *Details*. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Berichte-Bereichs des WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- SMTP
- SMTP-Profile
- POP3
- Email Encryption
- SPX-Verschlüsselung
- Quarantänebericht
- Mail-Manager

10.1 SMTP

Im Menü *Email Protection > SMTP* können Sie den SMTP-Proxy konfigurieren. SMTP ist die Abkürzung für *Simple Mail Transfer Protocol*, ein Protokoll, das zum Ausliefern von E-Mails an einen Mailserver verwendet wird. Sophos UTM besitzt ein Gateway auf Anwendungsebene für SMTP, das dazu genutzt werden kann, Ihren internen Mailserver vor Angriffen aus dem Internet zu schützen. Außerdem bietet es effektive Antivirenscan- und E-Mail-Filterungs-Dienste.

Hinweis – Damit der SMTP-Proxy korrekt funktioniert, muss ein gültiger Namensserver (DNS) konfiguriert sein.

10.1.1 Allgemein

Auf der Registerkarte *Email Protection > SMTP > Allgemein* können Sie festlegen, ob Sie für die Konfiguration von SMTP den *Einfachen Modus* oder den *Profilmodus* verwenden wollen.

1. **Aktivieren Sie SMTP.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und der Abschnitt *Konfigurationsmodus* kann nun bearbeitet werden.

2. **Wählen Sie einen Konfigurationsmodus.**
   Einfacher Modus: Verwenden Sie diesen Modus, falls alle Domänen dieselben Einstellungen teilen. Dennoch können Sie Ausnahmen definieren, die auf Domänennamen, E-Mail-Adressen und Hosts basieren. Es besteht keine Einschränkung in der Funktionalität im Vergleich zum *Profilmodus*.

   Profilmodus (nicht verfügbar mit BasicGuard-Abonnement): In diesem Modus können Sie globale Einstellungen überschreiben oder erweitern, z. B. für Antispam oder Antivirus, für individuelle Domänen oder Domänengruppen, indem Sie für diese Profile im Menü *SMTP-Profile* anlegen. Einstellungen, die im Menü *SMTP* vorgenommen wurden, gelten trotzdem noch für die ihnen zugeteilten Domänen und dienen außerdem als Standardeinstellungen für Profile. Wenn Sie den *Profilmodus* wählen, finden Sie zu einigen Einstellungen zusätzliche Hinweise mit Empfehlungen bezüglich des Profilmodus und zum Verhalten der UTM.

3. **Klicken Sie auf *Übernehmen*.**
   Der gewählte Modus wird aktiviert.

10.1.2 Routing

Auf der Registerkarte *Routing* können Sie Domänen- und Routingziele für den SMTP-Proxy konfigurieren. Außerdem können Sie festlegen, wie Empfänger verifiziert werden sollen.

Um das SMTP-Proxy-Routing zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Geben Sie Ihre interne(n) Domäne(n) ein.**
   Um E-Mail-Domänen einzugeben, klicken Sie auf das Plussymbol im Feld *Domänen*.

Geben Sie im angezeigten Textfeld die Domäne in der Form `beispiel.de` ein und klicken Sie auf *Übernehmen*. Wiederholen Sie diesen Schritt bis alle Domänen aufgeführt sind.

Im *Profilmodus*: Geben Sie nur Domänen ein, die globale Einstellungen verwenden. Alle anderen Domänen sollten in ihren jeweiligen Profilen aufgeführt sein.

2. **Geben Sie den internen Server an.**
   Wählen Sie aus der Auswahlliste *Routen nach* den Host aus, zu dem E-Mails für die oben aufgeführten Domänen weitergeleitet werden sollen. Ein üblicher Zielhost wäre der Microsoft Exchange Server in Ihrem lokalen Netzwerk. Sie können zwischen verschiedenen Servertypen wählen:

   - **Statische Hostliste:** Wählen Sie eine Hostdefinition der Zielroute aus dem Feld *Hostliste*. Beachten Sie, dass Sie mehrere Hostdefinitionen wählen können, um ein einfaches Failover gewährleisten zu können. Wenn die Zustellung an den ersten Host fehlschlägt, werden die Mails zum nächsten Host geroutet. Die (statische) Reihenfolge der Hosts kann in der aktuellen Version von Sophos UTM jedoch nicht festgelegt werden und ist etwas zufällig. Um die Zustellung zufällig auf eine Gruppe von Hosts zu verteilen und dadurch zusätzlich einen einfachen Lastausgleich zu erlangen, verwenden Sie den Routentyp *DNS-Hostname* und geben Sie einen Hostnamen an, der mehrere A-Einträge (engl. A Record) besitzt (ein *A-Eintrag* oder *Address Resource Record* bildet im DNS einen Hostnamen auf eine IP-Adresse ab).

   - **DNS-Hostname:** Geben Sie den *vollständigen Domänennamen* (FQDN, fully qualified domain name) Ihrer Zielroute an (z. B. `exchange.beispiel.de`). Beachten Sie, wenn Sie einen DNS-Namen mit mehreren A-Einträgen (engl. A Record) auswählen, werden die Mails an jeden Server beliebig verteilt. Wenn ein Server ausfällt, werden darüber hinaus alle Mails automatisch zu den verbleibenden Servern geroutet.

   - **MX-Einträge:** Sie können Mails auch über MX-Einträge (engl. MX Records) zu Ihre(r/n) Domäne(n) routen.Wenn Sie diesen Routentyp wählen, wird der Mail-Transfer-Agent von Sophos UTM eine DNS-Anfrage starten, um den MX-Eintrag vom Domänennamen des Empfängers zu erfragen. Das ist der Teil der E-Mail-Adresse, die nach dem „@“-Zeichen steht. Stellen Sie sicher, dass das Gateway nicht der primäre MX-Server für die oben angegebene Domäne ist, da er Mails nicht sich selbst zustellen wird.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Empfängerverifizierung

Empfänger verifizieren: Hier können Sie festlegen, ob und wie E-Mail-Empfänger verifiziert werden.

- **Mit Serveranfrage:** Es wird eine Anfrage an den Server geschickt, um den Empfänger zu verifizieren.
- **Im Active Directory:** Es wird eine Anfrage an den Active-Directory-Server geschickt, um den Empfänger zu verifizieren. Um Active Directory benutzen zu können, muss ein Active-Directory-Server unter *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Server* angegeben worden sein. Geben Sie einen BaseDN im Feld *Alternativer BaseDN* ein.

  Hinweis – Die Verwendung der Active-Directory-Empfängerverifizierung kann dazu führen, dass Nachrichten abgelehnt werden, wenn der Server nicht antwortet.

- **Aus:** Sie können die Empfängerverifizierung vollständig ausschalten, aber das ist nicht empfehlenswert, da es zu einem höheren Spam-Aufkommen und Wörterbuchangriffen führt. Dadurch erhöhen Sie die Wahrscheinlichkeit, dass Ihre Quarantäne mit unerwünschten Nachrichten „überflutet" wird.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

10.1.3 Antivirus

Die Registerkarte *Antivirus* bietet verschiedene Maßnahmen gegen E-Mails, die schädlichen oder gefährlichen Inhalt haben wie Viren, Würmer oder andere Schadsoftware.

Hinweis – Ausgehende E-Mails werden gescannt, wenn das Auswahlkästchen *Relay-Nachrichten (ausgehend) scannen* auf der Registerkarte *Relaying* markiert ist.

Während SMTP-Übermittlung scannen

Wählen Sie die Option *Schadsoftware während SMTP-Übermittlung ablehnen*, wenn Nachrichten bereits während der SMTP-Übermittlung gescannt werden und abgelehnt werden sollen, wenn sie Schadsoftware enthalten.

Im *Profilmodus*: Diese Einstellung kann nicht für einzelne Profile geändert werden. Bei Nachrichten mit mehr als einem Empfänger wird diese Funktion ausgesetzt, wenn bei einem der Empfängerprofile *Antiviren-Scan* ausgeschaltet ist. Das bedeutet, dass es sinnvoll ist, die reguläre Antiviren-Einstellung unten auf entweder *Verwerfen* oder *Quarantäne* gestellt zu lassen.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Antiviren-Scan

Wenn Sie diese Option wählen, werden E-Mails nach unerwünschtem Inhalt gescannt wie z. B. Viren, Trojanischen Pferden oder verdächtigen Dateitypen. Nachrichten mit schädlichem Inhalt werden blockiert oder in der E-Mail-Quarantäne gespeichert. Benutzer können ihre unter Quarantäne stehenden E-Mails ansehen und freigeben, entweder über das SophosBenutzerportal oder den täglichen Quarantänebericht. Nachrichten, die schädlichen Inhalt enthalten, können jedoch nur vom Administrator über den Mail-Manager aus der Quarantäne freigegeben werden.

Antivirus: Hier können Sie festlegen, wie mit Nachrichten verfahren wird, die schädlichen Inhalt besitzen. Die folgenden Aktionen sind möglich:

- **Aus:** Es werden keine Antiviren-Scans durchgeführt.
- **Verwerfen:** Eingehende Nachrichten werden angenommen und sofort gelöscht. Ausgehende Nachrichten werden nie verworfen, um unbeabsichtigten E-Mail-Verlust zu verhindern. Stattdessen werden sie in die Quarantäne verschoben.
- **Quarantäne:** Die Nachricht wird blockiert und in die E-Mail-Quarantäne verschoben. Nachrichten in Quarantäne können entweder über das Benutzerportal oder den täglichen Quarantänebericht eingesehen werden. Beachten Sie, dass Nachrichten mit schädlichem Inhalt nur vom Administrator aus der Quarantäne freigegeben werden können.

Sophos UTMbietet mehrere Antiviren-Mechanismen für höchste Sicherheit:

- **Einzelscan:** Standardeinstellung; bietet maximale Leistung. Die auf der Registerkarte *Systemeinstellungen* > *Scan-Einstellungen* festgelegte Engine wird verwendet.
- **Zweifachscan:** Bietet maximale Erkennungsrate, da der entsprechende Verkehr von zwei verschiedenen Virenscannern gescannt wird. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist.

Unscannbaren und verschlüsselten Inhalt in Quarantäne: Wählen Sie diese Option, um E-Mails unter Quarantäne zu stellen, deren Inhalt nicht gescannt werden konnte. Unscannbarer Inhalt können verschlüsselte Archive oder sehr große Inhalte sein, oder es kann ein technischer Grund vorliegen wie z. B. der Ausfall eines Scanners.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

MIME-Typ-Filter

Der MIME-Typ-Filter liest den Typ von E-Mail-Inhalten aus. Sie können festlegen, wie mit den verschiedenen MIME-Typen umgegangen werden soll.

- **Audioinhalte in Quarantäne:** Wenn Sie diese Option wählen, werden Audioinhalte wie mp3- oder wav-Dateien unter Quarantäne gestellt.
- **Videoinhalte in Quarantäne:** Wenn Sie diese Option wählen, werden Videoinhalte wie mpg- oder mov-Dateien unter Quarantäne gestellt.
- **Ausführbare Inhalte in Quarantäne:** Wenn Sie diese Option wählen, werden ausführbare Inhalte wie exe-Dateien unter Quarantäne gestellt.

Weitere Typen in Quarantäne: Um einen anderen MIME-Typ als die obigen hinzuzufügen, der unter Quarantäne gestellt werden soll, klicken Sie auf das Plussymbol im Feld *Weitere Typen in Quarantäne* und geben Sie den MIME-Typ an (z. B. `image/gif`). Sie können Platzhalter (`*`) auf der rechten Seite des Schrägstriches verwenden, z. B. `application/*`.

Inhaltstypen auf Whitelist: Sie können in dieses Feld MIME-Typen eintragen, die generell zugelassen sein sollen.Um einen MIME-Typ hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Inhaltstypen auf Whitelist* und geben Sie den MIME-Typ ein. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

<table>
<tr><th>MIME-Typ</th><th>MIME-Typ-Klasse</th></tr>
<tr><td>audio/*</td><td>Audiodateien</td></tr>
<tr><td>video/*</td><td>Videodateien</td></tr>
<tr><td>application/x-dosexec</td><td rowspan="9">Anwendungen</td></tr>
<tr><td>application/x-msdownload</td></tr>
<tr><td>application/exe</td></tr>
<tr><td>application/x-exe</td></tr>
<tr><td>application/dos-exe</td></tr>
<tr><td>vms/exe</td></tr>
<tr><td>application/x-winexe</td></tr>
<tr><td>application/msdos-windows</td></tr>
<tr><td>application/x-msdos-program</td></tr>
</table>

Tabelle 2: MIME-Typen, die dem MIME-Typ-Filter bekannt sind

Dateierweiterungenfilter

Mit dieser Funktion können Sie E-Mails unter Quarantäne stellen (mit Warnung), die bestimmte Dateitypen enthalten, basierend auf ihren Dateierweiterungen (z. B. ausführbare Dateien). Um Dateierweiterungen hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Blockierte Erweiterungen* und geben Sie eine kritische Dateierweiterung ein, die gesperrt werden soll, z. B. `exe` oder `jar` (ohne den Punkt als Trennzeichen). Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Archive können nicht auf verbotene Dateierweiterungen gescannt werden. Um Ihr Netzwerk vor Schadsoftware aus Archivdateien zu schützen, sollten Sie in Betracht ziehen, die entsprechenden Archivdateierweiterungen gänzlich zu blockieren.

Fußzeile über Antivirenprüfung

Jeder ausgehenden Nachricht können Sie eine spezielle Fußzeile hinzufügen beziehungsweise anpassen, die Benutzer darüber informiert, dass die E-Mail auf schädliche Inhalte gescannt wurde. Die Fußzeile wird jedoch nur hinzugefügt, wenn das Auswahlkästchen *Relay-Nachrichten (ausgehend) scannen* auf der Registerkarte *Relaying* markiert ist. Darüber hinaus wird die Antivirenprüfungsfußzeile nicht an die E-Mail angehängt, wenn es sich bei der E-Mail um eine Antwort handelt (d. h. sie besitzt den Header *In-Reply-To*) oder wenn die Inhaltsart der E-Mail nicht bestimmt werden konnte. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Das Hinzufügen einer Fußzeile durch ein E-Mail-Programm (z. B. Microsoft Outlook oder Mozilla Thunderbird) zu Nachrichten, die bereits signiert oder verschlüsselt sind, zerstört die Signatur der E-Mails und macht sie damit ungültig. Wenn Sie digitale Zertifikate Client-seitig erzeugen wollen, deaktivieren Sie die Fußzeile der Antivirenprüfung. Wenn Sie jedoch nicht auf Datenschutz und Authentifizierung in Ihrer E-Mail-Kommunikation verzichten möchten und dennoch eine allgemeine Fußzeile für die Antivirenprüfung verwenden wollen, sollten Sie die integrierte Email-Encryption-Funktion von Sophos UTM einsetzen. Bei der Email Encryption auf dem Gateway wird die Fußzeile vor der digitalen Signierung zur Nachricht hinzugefügt, wodurch die Signatur intakt bleibt.

10.1.4 Antispam

Sophos UTMkann so konfiguriert werden, dass es unerwünschte Spam-E-Mails entdeckt und Spam-Übermittlungen von bekannten oder verdächtigten Spam-Versendern identifiziert. Die Konfigurationsoptionen auf der Registerkarte *Antispam* ermöglichen die Konfiguration von SMTP-Sicherheitsfunktionen, die darauf ausgelegt sind, Ihr Netzwerk vor dem Empfang von unerwünschten kommerziellen E-Mails zu schützen.

Hinweis – Ausgehende E-Mails werden gescannt, wenn das Auswahlkästchen *Relay-Nachrichten (ausgehend) scannen* auf der Registerkarte *Relaying* markiert ist.

Hinweis – Einige der Funktionen auf dieser Registerkarte stehen mit dem BasicGuard-Abonnement nicht zur Verfügung.

Spam-Erkennung während SMTP-Übermittlung

Sie haben die Möglichkeit, Spam bereits zum Zeitpunkt der SMTP-Übermittlung abzulehnen. Wählen Sie eine der folgenden Einstellungen für die Option *Während SMTP-Übermittlung ablehnen*:

- **Aus:** Spam-Erkennung ist ausgeschaltet und es werden keine E-Mails aufgrund von Spamverdacht abgelehnt.
- **Bestätigten Spam:** Nur bestätigter Spam wird abgelehnt.
- **Spam:** Alle E-Mails, die das System für Spam hält, werden abgelehnt. Beachten Sie, dass hierbei die Rate der Fehlfunde (engl. false positives) steigen kann, da möglicherweise auch E-Mails wie beispielsweise Newsletter als Spam betrachtet werden.

E-Mails, die nicht während der SMTP-Übermittlung abgelehnt werden, werden entsprechend Ihrer Einstellungen im Bereich *Spamfilter* unten behandelt.

Im *Profilmodus*: Diese Einstellung kann nicht für einzelne Profile geändert werden. Nachrichten mit mehr als einem Empfänger lassen diese Funktion aus, wenn bei einem der Empfängerprofile der Spam-Scan ausgeschaltet ist. Das bedeutet, dass es sinnvoll ist, die reguläre Einstellung zur Spam-Erkennung entweder auf *Spam* oder *Bestätigten Spam* eingestellt zu lassen.

RBLs (Echtzeit-Blackhole-Listen)

Echtzeit-Blackhole-Listen (Realtime Blackhole Lists, RBL) sind eine Methode, mit der Websites eine Liste von IP-Adressen bekannt geben, die mit Spam-Versand in Verbindung gebracht werden.

Empfohlene RBLs verwenden: Die Wahl dieser Option sorgt dafür, dass externe Datenbanken nach bekannten Spam-Versendern (sogenannten *Echtzeit-Blackhole-Listen*) abgefragt werden. Nachrichten, die von einer Domäne gesendet werden, die in einer oder mehrerer dieser Listen aufgeführt ist, können einfach abgelehnt werden. Es sind einige Dienste dieser Art im Internet verfügbar. Diese Funktion ist eine enorme Hilfe bei der Reduzierung des Spam-Aufkommens.
Standardmäßig werden die folgenden RBLs abgefragt:

- Commtouch IP Reputation (ctipd.org)
- cbl.abuseat.org

Hinweis – Die RBLs, die von Sophos UTM abgefragt werden, können sich ohne Ankündigung ändern. Sophosübernimmt keine Gewähr für den Inhalt dieser Datenbanken.

Sie können weitere RBL-Sites hinzufügen, um die Antispam-Fähigkeiten von Sophos UTM zu verbessern. Klicken Sie dazu auf das Plussymbol im Feld *Extra-RBL-Zonen*. Geben Sie die RBL-Zone in das angezeigte Textfeld ein.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Spamfilter

Sophos UTMbietet eine heuristische Prüfung von E-Mails auf Spam-Eigenschaften. Sie benutzt dafür SMTP-Envelope-Informationen (envelope = Umschlag) und eine interne Datenbank mit heuristischen Tests und Eigenschaften. Die Spamfilter-Option bewertet Nachrichten basierend auf ihrem Inhalt und SMTP-Envelope-Informationen. Höhere Werte deuten auf eine höhere Spam-Wahrscheinlichkeit hin.

Mit den folgenden beiden Optionen können Sie festlegen, was mit Nachrichten geschehen soll, denen ein gewisser Spam-Wert zugewiesen wurde. So wird sichergestellt, dass potenzielle Spam-E-Mails vom Gateway anders behandelt werden.

- **Spam-Aktion:** Hier können Sie festlegen, was mit Nachrichten geschieht, die als möglicher Spam eingestuft wurden. Beachten Sie, dass es Fehlfunde geben kann, z. B.

Newsletter, und daher durch Verwerfen E-Mails verloren gehen können.

- **Aktion bei bestätigtem Spam:** Hier können Sie festlegen, was mit Nachrichten geschieht, die sicher Spam sind.

Sie können zwischen verschiedenen Aktionen für diese beiden Arten von Spam wählen:

- **Aus:** Es werden keine Nachrichten als Spam markiert oder ausgefiltert.
- **Warnen:** Es werden keine Nachrichten herausgefiltert. Stattdessen wird bei eingehenden Nachrichten eine Spam-Markierung („Flag“) zum Header der Nachricht hinzugefügt und der Betreff der Nachricht erhält eine Spam-Kennzeichnung. Auf ausgehende Nachrichten wird keine Aktion angewendet.
- **Quarantäne:** Die Nachrichten werden blockiert und in die E-Mail-Quarantäne verschoben. Nachrichten in Quarantäne können entweder über das Benutzerportal oder den täglichen Quarantänebericht eingesehen werden.
- **Verwerfen:** Eingehende Nachrichten werden angenommen und sofort gelöscht. Ausgehende Nachrichten werden nie verworfen, um unbeabsichtigten E-Mail-Verlust zu verhindern. Stattdessen werden sie in die Quarantäne verschoben.

Spam-Kennzeichnung: Mit dieser Option können Sie eine Kennzeichnung für Spam-Nachrichten festlegen, d. h., dass eine Zeichenkette zur Betreffzeile der Nachricht hinzugefügt wird, die es einfach macht, Spam-Nachrichten schnell als solche zu erkennen. Standardmäßig wird die Zeichenkette `*SPAM*` benutzt, um Nachrichten als Spam zu kennzeichnen.

Absender-Blacklist

Der Envelope-Absender eingehender SMTP-Sitzungen wird mit den Adressen auf dieser Blacklist (Negativliste) verglichen. Wenn der Envelope-Absender auf der Blacklist gefunden wird, wird die Nachricht verworfen.
Um ein neues Adressmuster zur Blacklist hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Adressmuster auf Blacklist*, geben Sie eine (oder einen Teil einer) Adresse ein und klicken Sie *Übernehmen*.Sie können einen Asterisk (*) als Platzhalter verwenden, z. B. `*@abbeybnknational.com`.

> **Tipp –** Endbenutzer können im Benutzerportal ihre eigenen Black- und Whitelisten anlegen.

Ausdruckfilter

Der Ausdruckfilter prüft den Inhalt von Nachrichten, die den SMTP-Proxy passieren, auf bestimmte Ausdrücke. Verdächtige E-Mails werden blockiert. Ausdrücke können in Form von *Perl Compatible Regular Expressions* (Perl-kompatible reguläre Ausdrücke) eingegeben

werden. Einfache Zeichenfolgen wie „Online Dating“ werden ohne Berücksichtigung der Groß-/Kleinschreibung interpretiert. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Querverweis – Detaillierte Informationen zur Verwendung von regulären Ausdrücken im Ausdruckfilter finden Sie in der Sophos-Knowledgebase.

Erweiterte Antispam-Funktionen

Dieser Abschnitt enthält weitere Optionen, die die Antispam-Fähigkeiten von Sophos UTM verbessern.

Ungültige HELO/fehlende RDNS ablehnen: Wählen Sie diese Option, wenn Sie Hosts ablehnen wollen, die ungültige HELO-Einträge senden oder bei denen RDNS-Einträge fehlen. Wenn Sie Hosts von dieser Prüfung ausnehmen wollen, benutzen Sie die entsprechende Option auf der Registerkarte *Ausnahmen*.

> **Strikte RDNS-Prüfung durchführen:** Wählen Sie diese Option, wenn Sie zusätzlich E-Mails von Hosts mit ungültigen RDNS-Einträgen ablehnen wollen. Ein RDNS-Eintrag ist ungültig, wenn der gefundene Hostname sich nicht zurück zur ursprünglichen IP-Adresse auflösen lässt.

Greylisting verwenden: Greylisting (dt. Verwendung grauer Listen) bedeutet, dass E-Mails für einen gewissen Zeitraum abgelehnt werden. Ein Mailserver, der Greylisting verwendet, speichert üblicherweise die folgenden Informationen von allen eingehenden Nachrichten:

- Absenderadresse
- IP-Adresse des Hosts, der die Nachricht verschickt hat
- Empfängeradresse
- Betreff der Nachricht

Diese Daten werden mit der internen Datenbank des SMTP-Proxy verglichen. Wenn die Daten noch nicht vorhanden sind, wird ein Eintrag in die Datenbank geschrieben, zusammen mit einem speziellen Zeitstempel, der die Daten beschreibt. Dieser Datensatz bewirkt, dass die E-Mail für einen Zeitraum von fünf Minuten abgelehnt wird. Nach diesem Zeitraum ist der Datensatz dem Proxy bekannt und die Nachricht wird beim nächsten Zustellversuch akzeptiert. Beachten Sie, dass der Datensatz nach einer Woche verfällt, wenn er innerhalb dieses Zeitraums nicht aktualisiert wird.
Greylisting nutzt die Tatsache, dass die meisten Versender von Spam-Mails Software verwenden, die nach der „Fire-and-Forget“-Methode arbeiten: Versuche die E-Mail zuzustellen

und wenn es nicht klappt, vergiss es! Das heißt, dass die Versender solcher Spam-Mails nicht wie RFC-konforme Mailserver versuchen, die Mail bei einem vorübergehenden Fehlschlag nochmals zu versenden. Da in der RFC-Spezifikation vorgesehen ist, dass die E-Mail-Zustellung vorübergehend fehlschlagen kann, geht Greylisting davon aus, dass ein legitimer Server es noch einmal versuchen wird und der Zielhost dann die E-Mails annimmt.

BATV verwenden: BATV (Bounce Address Tag Validation) ist ein Entwurf des Standardisierungsgremiums Internet Engineering Task Force (IETF), bei dem der Versuch unternommen wird, die legitime Benutzung von E-Mail-Adressen von unautorisierter Benutzung zu unterscheiden. BATV bietet eine Methode, den Envelope-Sender von ausgehenden Mails zu signieren, indem ein einfacher geteilter Schlüssel hinzugefügt wird, der einen Hash der Adresse und zeitvariante Informationen sowie einige zufällige Daten codiert. Prinzipiell wird es dazu benutzt, Ablehnungsnachrichten (engl. bounce messages) abzuweisen, die nicht von Ihnen versendet wurden. Durch BATV können Sie nun herausfinden, ob Ablehnungsnachrichten, die Sie erhalten, wirklich durch eine von Ihnen versendete Mail ausgelöst wurden oder nicht durch einen Spam-Versender, der eine E-Mail mit Ihrer Adresse gefälscht hat. Wenn eine Ablehnungsnachricht eintrifft und die E-Mail ist nicht nach BATV signiert, wird der SMTP-Proxy die Nachricht nicht annehmen. Beachten Sie, dass die BATV-Signatur nach sieben Tagen abläuft. Um den Schlüssel (auch *BATV-Secret* genannt) zu ändern, der für die Verschlüsselung des Hashes der Envelope-Adresse `MAIL FROM` verwendet wird, gehen Sie zur Registerkarte *Email Protection > SMTP > Erweitert*.

> **Hinweis –** Einige Mail-Transfer-Programme (Mail Transfer Agents, MTA) könnten E-Mails zurückweisen, deren Envelope-Absenderadresse mittels BATV verändert wurde. In diesem Fall müssen Sie für die betroffenen Absenderadressen, Empfängeradressen oder Domänen eine entsprechende Ausnahmeregel definieren.

SPF-Prüfung durchführen: SPF (*Sender Policy Framework*) ist ein System bei dem Domäneninhaber Informationen über ihre Mailserver für ausgehende Mails veröffentlichen können. Domänen benutzen öffentliche Einträge, um Anfragen nach verschiedenen Diensten (Web, E-Mail, usw.) an jene Hosts weiterzuleiten, die diese Dienste anbieten. Alle Domänen veröffentlichen MX-Einträge für E-Mail-bezogene Dienste, damit andere wissen, welche Hosts E-Mails für die Domäne entgegennehmen. SPF funktioniert durch Domänen, die zusätzlich eine Art „Rückwärts-MX“ veröffentlichen, um der Welt mitzuteilen, welche Hosts E-Mails von welcher Domäne versenden. Wenn der Empfänger eine Nachricht von einer bestimmten Domäne erhält, kann er diese Einträge überprüfen, um sicherzustellen, dass die E-Mail wirklich daher kommt, woher sie kommen soll.

Querverweis – Weitere Informationen erhalten Sie auf der Internetseite zu Sender Policy Framework.

Als zusätzliche Antispam-Funktion vergleicht der SMTP-Proxy stillschweigend jede Empfängeradresse, die er erhält, mit Ihrem Backend-Mailserver, bevor er die Mail für diese Adresse annimmt.E-Mails für ungültige Empfängeradressen werden nicht angenommen. Damit die Funktion greift, muss/müssen Ihr(e) Backend-Mailserver E-Mails von unbekannten Empfängern zur SMTP-Zeit ablehnen. Die Grundregel lautet: Wenn Ihr Backend-Server eine Nachricht ablehnt, lehnt sie der SMTP-Proxy ebenfalls ab.

Beachten Sie jedoch, dass die Empfängerüberprüfung *nicht* für vertrauenswürdige (authentifizierte) Hosts oder Relay-Hosts durchgeführt wird, da manche Benutzerprogramme (User Agents) ein Problem damit haben, wenn Empfänger während der SMTP-Übertragung abgelehnt werden. Gewöhnlich (der Backend-Mailserver lehnt unbekannte Empfänger während der SMTP-Übertragung ab) wird Sophos UTM E-Mails nur in den folgenden Fällen ablehnen (bounce):

- Wenn eine vertrauenswürdige Quelle oder ein Relay-Host eine Nachricht zu einem nicht verfügbaren Empfänger sendet.
- Wenn der Backend-Mailserver nicht erreichbar war, sodass Sophos UTM den Empfänger nicht verifizieren konnte.

Jedoch hindert Sophos UTM Ihre(n) Backend-Mailserver nicht daran, NDRs (non-delivery reports, Berichte über Nicht-Auslieferung) oder Ablehnungsnachrichten (bounces) zu versenden. Zudem speichert Sophos UTM Callout-Antworten des Mailservers zwischen: positive Antworten 24 Stunden lang und negative zwei Stunden.

10.1.5 Datenschutz

Auf der Registerkarte *SMTP > Data Protection* ermöglicht die Funktion „Data Protection“ eine Reduzierung des zufälligen Datenverlusts von Workstations, indem die Übertragung von Dateien, die vertrauliche Daten enthalten, überwacht und eingeschränkt wird. Zufälliger Datenverlust wird häufig durch Mitarbeiter verursacht, die nicht richtig mit vertraulichen Daten umgehen. Beispiel: Ein Benutzer schickt sich eine Datei mit vertraulichen Informationen per E-Mail (SMTP) nach Hause. Data Protection scannt ausgehende E-Mails einschließlich Betreffzeile, Textkörper und Anhängen auf vertrauliche Informationen. Je nach Ergebnis kann die E-Mail mithilfe von SPX-Verschlüsselung verschlüsselt oder die E-Mail kann abgelehnt oder gesendet werden.

Legen Sie die Einstellungen in den folgenden Abschnitten fest, um Data Protection zu konfigurieren.Solange keine Sophos-Inhaltssteuerregel ausgewählt ist und keine benutzerdefinierte Regel festgelegt wurde, ist diese Funktion deaktiviert.

Datenschutzrichtlinie

Anhänge scannen: Bei Auswahl dieser Option werden die Anhänge zusätzlich zur Nachricht selbst auf vertrauliche Daten gescannt.

Aktion bei Regelübereinstimmung: Wählen Sie aus, wie eine E-Mail bei Auslösung der Richtlinie behandelt wird:

> **Ablehnen:** Eine E-Mail, welche die Richtlinie auslöst, wird nicht gesendet.
>
> **Mit SPX-Verschlüsselung senden:** Eine E-Mail, welche die Richtlinie auslöst, wird automatisch mit SPX-Verschlüsselung gesendet (siehe Registerkarte *Email Protection > SPX-Verschlüsselung*).Falls SMTP im einfachen Modus verwendet wird, wird die SPX-Vorlage, die auf der Registerkarte *SMTP > Allgemein* ausgewählt ist, für die SPX-Verschlüsselung verwendet.Falls SMTP im Profilmodus verwendet wird, hängt die verwendete SPX-Vorlage vom SMTP-Profil ab, das der Domäne des Absenders zugewiesen wurde (siehe Registerkarte *SMTP-Profile*).Falls die Domäne des Absenders keinem Profil zugewiesen ist, wird die Standardvorlage verwendet, die unter der Registerkarte *SMTP > Allgemein* ausgewählt wurde.
>
> **Zulassen:** Eine E-Mail, welche die Richtlinie auslöst, wird trotzdem gesendet.

Bei Übereinstimmung benachrichtigen: Wählen Sie aus, ob der Absender der E-Mail, der Administrator und/oder sonstige Personen benachrichtigt werden sollen. Für die Benachrichtigung sonstiger Personen müssen Sie die entsprechende E-Mail-Adresse angeben.Der Text der E-Mail-Benachrichtigung kann über die Registerkarte *Verwaltung > Anpassungen > E-Mail-Nachrichten* angepasst werden.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Sophos-Inhaltssteuerungsregeln

Art: Wählen Sie einen Eintrag aus der Auswahlliste, um die Anzahl der angezeigten Regeln entsprechend zu verringern.

Region: Wählen Sie einen Eintrag aus der Auswahlliste, um die Anzahl der angezeigten Regeln entsprechend zu verringern.

Nur ausgewählte anzeigen: Bei Aktivierung dieser Option werden nur ausgewählte Regeln in der Liste angezeigt.

Regeln: Wählen Sie die Regeln aus, die Sie für die Funktion Data Protection verwenden möchten. Wenn Sie mit dem Mauszeiger über einen Eintrag fahren, wird ein Tooltip mit zusätzlichen Informationen zur Regel angezeigt.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Benutzerdefinierte Regeln

Benutzerdefinierte Ausdrücke: Geben Sie die Ausdrücke ein, die Data Protection zusätzlich zu den oben ausgewählten Regeln verwenden soll. Sie können reguläre Ausdrücke hinzufügen.

> **Querverweis –** Detaillierte Informationen zur Verwendung von regulären Ausdrücken finden Sie hier, siehe Sophos-Knowledgebase.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

10.1.6 Ausnahmen

Auf der Registerkarte *SMTP* > *Ausnahmen* können Sie vertrauenswürdige Hosts, Netzwerke, Absender und Empfänger definieren, die dann von Antivirus-, Antispam- und anderen Sicherheitsprüfungen ausgenommen werden.

> **Hinweis –** Da E-Mails mehrere Empfänger haben können und Sophos UTM den Scan für das SMTP-Protokoll inline ausführt, wird die Überprüfung einer E-Mail gänzlich ausgesetzt, sobald einer der Empfänger der E-Mail im Feld *Empfänger* aufgeführt ist.

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahmenliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Ausnahme ein.

   Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, die nicht durchgeführt werden sollen. Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antivirus*, *Antispam* und *Data Protection*.

Für diese Quellhosts/-netzwerke: Wählen Sie die Quellhosts/-netzwerke (d. h. die Hosts oder Netzwerke, die Nachrichten senden), die gemäß dieser Ausnahmeregel von den Sicherheitsprüfungen ausgenommen werden sollen, oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Hinweis – Für Localhost muss keine Ausnahmeregel angelegt werden, da lokale Nachrichten standardmäßig nicht gescannt werden.

Wenn Sie diese Option wählen, wird das Feld *Hosts/Netzwerke* geöffnet. Hier können Sie einen Host oder ein Netzwerk eingeben, indem Sie auf das Plussymbol oder das Ordnersymbol klicken.

ODER Diese Empfängeradressen: Wählen Sie die Absenderadressen, die von den gewählten Sicherheitsprüfungen ausgenommen werden sollen.
Wenn Sie diese Option wählen, wird das Feld *Absender* geöffnet. Sie können entweder eine vollständige, gültige E-Mail-Adresse eingeben (z. B. `mmustermann@beispiel.de`) oder alle E-Mail-Adressen einer bestimmten Domäne, wobei Sie einen Asterisk (*) als Platzhalter verwenden (z. B. `*@beispiel.de`).

Hinweis – Verwenden Sie die *Absender*-Option mit Vorsicht, da Absenderadressen leicht gefälscht werden können.

ODER Diese Empfängeradressen: Wählen Sie die Empfängeradressen, die von den gewählten Sicherheitsprüfungen ausgenommen werden sollen.

Wenn Sie diese Option wählen, wird das Feld *Empfänger* geöffnet. Sie können entweder eine vollständige, gültige E-Mail-Adresse eingeben (z. B. `mmustermann@beispiel.de`) oder alle E-Mail-Adressen einer bestimmten Domäne, wobei Sie einen Asterisk (*) als Platzhalter verwenden (z. B. `*@beispiel.de`).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

10.1.7 Relaying

Der SMTP-Proxy kann als Mail-Relay konfiguriert werden.Ein Mail-Relay ist ein SMTP-Server, der so konfiguriert ist, dass er bestimmten Benutzern, Benutzergruppen oder Hosts erlaubt, E-Mails durch ihn an Domänen hindurchzuleiten, die lokal nicht erreichbar sind.

Hinweis – Einige der Funktionen auf dieser Registerkarte stehen mit dem BasicGuard-Abonnement nicht zur Verfügung.

Upstream-Host-Liste

Ein Upstream-Host ist ein Host, der E-Mails an Sie weiterleitet, z. B. Ihr ISP oder externer MX. Wenn Sie eingehende E-Mails von statischen Upstream-Hosts erhalten, ist es nötig, dass Sie diese Hosts hier eintragen. Andernfalls wird der Spamschutz nicht richtig funktionieren.

Um einen Upstream-Host hinzuzufügen, klicken Sie entweder auf das Plussymbol oder auf das Ordnersymbol, um Hosts direkt aus der *Netzwerke*-Objektleiste zu ziehen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert. Wenn Sie ausschließlich Upstream-Hosts zulassen möchten, wählen Sie die Option *Nur Upstream/Relay-Hosts zulassen*. Der SMTP-Zugriff wird dann auf die definierten Upstream-Hosts begrenzt. Upstream-Hosts können sich authentifizieren, um Relaying-Rechte zu erhalten. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Authentifiziertes Relay

SMTP-Clients können sich authentifizieren, um Relaying-Rechte zu erlangen. Wählen Sie die Option *Authentifiziertes Relaying* zulassen und geben Sie die Benutzer oder Benutzergruppen an, die diese Funktion verwenden dürfen. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Wenn das Auswahlkästchen *Nur Upstream/Relay-Hosts zulassen* markiert ist, funktioniert *Authentifiziertes Relay* nur, wenn der sendende Host als Upstream- oder Relay-Host konfiguriert ist.

Hostbasiertes Relay

Mail-Relaying kann auch hostbasiert ablaufen. Wenn Ihr lokaler Mailserver oder Ihre Mail-Clients in der Lage sein sollen, den SMTP-Proxy als Mail-Relay zu verwenden, müssen Sie die

Netzwerke und Hosts, die E-Mails über das Relay versenden dürfen, zum Feld *Zugelassene Hosts/Netzwerke hinzufügen*. Die aufgeführten Netzwerke und Hosts dürfen Nachrichten an beliebige Adressen versenden. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Warnung – Wählen Sie im Feld *Zugelassene Hosts/Netzwerke* niemals *Any* aus, denn das würde zu einem offenen Mail-Relay führen, welches es jedem aus dem Internet gestattet, Nachrichten über den SMTP-Proxy zu senden. Spam-Versender werden das schnell herausfinden und das wird zu einem erheblichen E-Mail-Aufkommen führen. Im schlimmsten Fall werden Sie auf Spam-Versender-Negativlisten (Blacklists) Dritter geführt. In den meisten Konfigurationen sind die einzigen Hosts, die als Mail-Relay agieren dürfen, die Mailserver in Ihrem Netzwerk.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Host-/Netzwerk-Blacklist

Hier können Sie Hosts und Netzwerke bestimmen, die vom SMTP-Proxy blockiert werden sollen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Inhaltsscan für (ausgehende) Relay-Nachrichten

Wenn diese Option gewählt ist, werden auch Nachrichten auf schädlichen Inhalt gescannt, die von authentifizierten oder hostbasierten Relays gesendet werden. Beim Versand vieler ausgehender Nachrichten kann das Ausschalten dieser Option ggf. die Leistung verbessern. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Beachten Sie, dass die globalen Antiviren- und Antispam-Einstellungen auch für ausgehende Nachrichten gelten. Unabhängig von diesen Einstellungen werden infizierte oder Spam-Nachrichten niemals verworfen, sondern unter Quarantäne gestellt, um den unbeabsichtigten Verlust von E-Mails zu vermeiden.

10.1.8 Erweitert

Auf der Registerkarte *SMTP > Erweitert* können Sie zusätzliche Sicherheitsoptionen für den SMTP-Proxy konfigurieren, unter anderem Smarthost-Einstellungen oder Transparenzmodus-Ausnahmen.

Übergeordneter Proxy

Ein übergeordneter Proxy (auch Parent oder Upstream Proxy) wird in Ländern benötigt, in denen der Zugang zum Internet nur über einen staatlich kontrollierten Proxy erlaubt ist. Falls Ihre Sicherheitsbestimmungen die Nutzung eines übergeordneten Proxys erforderlich machen, so können Sie diesen hier durch Angabe einer Hostdefinition und eines Ports konfigurieren.

Übergeordneten Proxy verwenden: Wählen Sie diese Option, um einen übergeordneten Proxy zu verwenden. Wählen Sie den Host aus oder fügen Sie einen Host hinzu und geben Sie den Proxy-Port ein. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort hier ein.

Transparenzmodus

Um den Transparenzmodus für SMTP zu aktivieren, markieren Sie das Auswahlkästchen und klicken Sie auf *Übernehmen*.
Hosts und Netzwerke, die im Feld *Hosts/Netze vom Transparenzmodus ausnehmen* aufgeführt sind, werden vom SMTP-Proxy nicht transparent überwacht. Um jedoch SMTP-Verkehr für diese Hosts und Netzwerke zuzulassen, wählen Sie die Option *SMTP-Verkehr für aufgeführte Hosts/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezielle Firewallregeln für die hier aufgeführten Hosts und Netzwerke anlegen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

TLS-Einstellungen

TLS-Zertifikat: Wählen Sie aus der Auswahlliste ein Zertifikat zum Aushandeln der TLS-Verschlüsselung mit allen Gegenstellen aus, die TLS unterstützen. Auf der Registerkarte *Site-to-Site-VPN > Zertifikatverwaltung > Zertifikate* können Sie Zertifikate erstellen oder hochladen.

Hosts/Netze, die TLS-Aushandlung erfordern: Fügen Sie hier Hosts oder Netze hinzu, die für die E-Mail-Kommunikation immer TLS-Verschlüsselung erfordern. Die UTM hält dann E-Mails zurück, wenn für diese Hosts/Netze keine TLS-Verschlüsselung zur Verfügung steht. Diese Nachrichten bleiben in der Mail-Warteschlange, bis TLS wieder verfügbar ist. Bleibt TLS über einen bestimmten Zeitraum nicht verfügbar, werden keine weiteren Versuche mehr unternommen, die E-Mail zu versenden, und der Benutzer erhält eine Benachrichtigung darüber, dass seine Nachricht nicht zugestellt werden konnte.

Absenderdomänen, die TLS-Verschlüsselung erfordern: Geben Sie hier die Domänen an, für die Sie eine TLS-Verschlüsselung für eingehende E-Mails erzwingen möchten. Von diesen Domänen versendete E-Mails ohne TLS werden umgehend zurückgewiesen.

Kein TLS für diese Hosts/Netze: Falls ein bestimmter Host oder ein Netzwerk Probleme mit TLS-Verschlüsselung hat, können Sie diesen/dieses im Feld angeben und das entsprechende TLS-Zertifikat aus der Auswahlliste auswählen. Dadurch nimmt die UTM den entsprechenden Host oder das entsprechende Netzwerk von der TLS-Aushandlung aus. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

DomainKeys Identified Mail (DKIM)

DKIM ist eine Methode, um ausgehende Nachrichten kryptografisch zu signieren. Um DKIM-Signierung zu verwenden, geben Sie Ihren privaten RSA-Schlüssel und den dazugehörigen Schlüsselselektor (key selector), den Schlüsselnamen, in die entsprechenden Felder ein. Fügen Sie dann die Domänen, für die Sie E-Mails signieren wollen, zum Feld *DKIM-Domänen* hinzu. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Vertraulichkeitsfußzeile

Sie können jeder ausgehenden E-Mail eine Vertraulichkeitsfußzeile hinzufügen, die Benutzer zum Beispiel darüber informiert, dass die E-Mail vertrauliche oder schutzwürdige Informationen enthalten kann, und sie anpassen. Die Vertraulichkeitsfußzeile wird jedoch nicht an die E-Mail angehängt, wenn es sich bei der E-Mail um eine Antwort handelt (d. h. sie besitzt den Header *In-Reply-To*) oder wenn die Inhaltsart der E-Mail nicht bestimmt werden konnte.

> **Hinweis –** Das Hinzufügen einer Fußzeile durch ein E-Mail-Programm (z. B. Microsoft Outlook oder Mozilla Thunderbird) zu Nachrichten, die bereits signiert oder verschlüsselt sind, zerstört die Signatur der E-Mails und macht sie damit ungültig. Wenn Sie digitale Zertifikate Client-seitig erzeugen wollen, deaktivieren Sie die Fußzeile der Antivirenprüfung. Wenn Sie jedoch nicht auf Datenschutz und Authentifizierung in Ihrer E-Mail-Kommunikation verzichten möchten und dennoch eine allgemeine Fußzeile für die Antivirenprüfung verwenden wollen, sollten Sie die integrierte Email-Encryption-Funktion von Sophos UTM einsetzen. Bei der Email Encryption auf dem Gateway wird die Fußzeile vor der digitalen Signierung zur Nachricht hinzugefügt, wodurch die Signatur intakt bleibt.

Erweiterte Einstellungen

Hier können Sie unter anderem den SMTP-Hostnamen und die Postmaster-Adresse einstellen.

SMTP-Hostname: Wenn ein SMTP-Hostname definiert ist, wird der SMTP-Proxy diesen Namen in HELO- und in SMTP-Banner-Nachrichten verwenden. Standardmäßig ist der Hostname des Systems angegeben.

Postmaster-Adresse: Tragen Sie die E-Mail-Adresse des Postmasters, des E-Mail-Verantwortlichen, für die UTM ein, an den die Nachrichten weitergeleitet werden, die in der Form `postmaster@[192.168.16.8]` gesendet werden, wobei die IP-Adresse eine der IP-Adressen der UTM ist. Die Annahme solcher Nachrichten ist eine RFC-Anforderung.

BATV-Schlüssel: Hier können Sie den automatisch generierten BATV-Schlüssel (engl. BATV secret) ändern, der vom SMTP-Proxy benutzt wird. Der BATV-Schlüssel ist ein verteilter Schlüssel, der verwendet wird, um die Envelope-Adresse (dt. Umschlagadresse) `MailFrom` einer E-Mail zu signieren, wodurch die Erkennung ungültiger Absenderadressen von Ablehnungsnachrichten möglich wird. Wenn Sie mehrere MXs für Ihre Domänen verwenden, können Sie den BATV-Schlüssel ändern, damit er auf allen Systemen gleich ist.

Max. Nachrichtengröße: Die maximale Größe der E-Mails, die vom Proxy akzeptiert wird. Diese Einstellung bezieht sich sowohl auf eingehende als auch auf ausgehende E-Mails. Falls Ihr Backend-Server eine Begrenzung in Bezug auf die Größe von E-Mails hat, dann sollten Sie hier denselben oder einen niedrigeren Wert einstellen.

Max. Verbindungen: Die maximale Anzahl gleichzeitiger Verbindungen, die der Proxy zulässt. Der Standardwert ist 20.

Max. Verbindungen/Host: Die maximale Anzahl an Verbindungen pro Host, die der Proxy zulässt. Der Standardwert ist 10.

Max. Mails/Verbindung: Die maximale Anzahl an Mails pro Verbindung, die der Proxy zulässt. Der Standardwert ist 1000.

Max. Empfänger/Mail: Die maximale Anzahl an Empfängern pro Mail, die der Proxy zulässt. Der Standardwert ist 100.

Fußzeilen-Modus: Hier können Sie bestimmen, wie Fußzeilen zu E-Mails hinzugefügt werden. *MIME-Teil* fügt die Fußzeile als Extra-MIME-Teil hinzu. Bereits vorhandene Teil-Encodierungen werden nicht geändert und sprachspezifische Sonderzeichen bleiben erhalten. Die andere Methode ist *Inline*, bei der die Fußzeile von der eigentlichen Mail durch das Trennzeichen `--` getrennt ist. Bei diesem Modus können Sie wählen, ob die Fußzeile nach Unicode (UTF-8) konvertiert wird oder nicht. Eine Unicode-Umwandlung verändert die Nachricht dahingehend, dass sprachspezifische Sonderzeichen in der Fußzeile erhalten bleiben.

Smarthost-Einstellungen

Ein Smarthost ist eine Art Mail-Relay-Server, der es einem SMTP-Server erlaubt, Mails an einen Upstream-Mailserver zu routen statt direkt an den Server des Empfängers. So ein Smarthost verlangt meistens, dass der Absender sich authentifiziert, um sicherzustellen, dass der Absender auch die Berechtigung besitzt, Mails durch den Smarthost weiterzuleiten.

Smarthost verwenden: Wenn Sie einen Smarthost für den Mailversand verwenden wollen, markieren Sie dieses Auswahlkästchen. In diesem Fall wird der Proxy Mails nie selbst zustellen, sondern diese immer an den Smarthost senden.

- **Smarthost:** Wählen Sie ein Smarthost-Objekt aus oder fügen Sie eins hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.
- **Smarthost-Port:** Der Standardport für die Smarthost-Verbindung ist 25. Falls notwendig, können Sie diesen Port ändern.
- **Dieser Smarthost erfordert Authentifizierung:** Wählen Sie diese Option, wenn der Smarthost Authentifizierung erfordert. Als Authentifizierungsmethode wird sowohl *Plain* als auch *Login* unterstützt. Geben Sie einen Benutzernamen und ein Kennwort in die entsprechenden Textfelder ein.

10.2 SMTP-Profile

Der SMTP-Proxy von Sophos UTM ermöglicht es Ihnen, alternative SMTP-Profile für verschiedene Domänen anzulegen. Auf diese Weise können Sie Domänen bestimmen, die ein anderes Profil verwenden sollen als das Standardprofil, das unter *Email Protection* > *SMTP* konfiguriert ist. Die Reihenfolge der Funktionen, die in Form von Registerkarten dargestellt sind, spiegelt die Abfolge einzelner Schritte während der SMTP-Zeit wider.

Um ein SMTP-Profil anzulegen, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den SMTP-Profilmodus.**
   Wählen Sie auf der Registerkarte *Email Protection > SMTP > Allgemein* die Option *Profilmodus* und klicken Sie auf *Übernehmen*.

   Das Anlegen von SMTP-Profilen im Menü *Email Protection > SMTP-Profile* ist aktiviert.
2. **Klicken Sie auf der Registerkarte *SMTP-Profile* auf *Neues Profil*.**
   Ein Dialogfeld wird geöffnet.
3. **Geben Sie einen aussagekräftigen Namen für das Profil an.**

4. **Fügen Sie eine oder mehrere Domänen hinzu.**
   Geben Sie im Feld *Domänen* eine oder mehrere Domänen an.

   Die Einstellungen dieses Profils gelten für diese Domänen.

5. **Nehmen Sie die folgenden Einstellungen vor:**
   Sie brauchen nur die Einstellungen für jene Funktionen vorzunehmen, die Sie verwenden wollen.Für jede der folgenden Funktionen können Sie entscheiden, ob die hier vorgenommenen individuellen Einstellungen verwendet werden sollen oder die globalen Einstellungen von *Email Protection* > *SMTP*. Standardmäßig ist die in den globalen Einstellungen gewählte Option ausgewählt. Die individuellen Einstellungen für jede Funktion sind unten beschrieben.

   Hinweis – Verschlüsselte E-Mails, deren Absenderadresse einen Domänennamen enthält, der hier konfiguriert ist, können nicht entschlüsselt werden, wenn Sie die E-Mail-Encryption-/Decryption-Funktion von Sophos UTM verwenden. Aus diesem Grund sollten Sie keine Profile für externe E-Mail-Domänen anlegen.

   Alle Einstellungen, die Sie hier vornehmen können, können unter *Email Protection* > *SMTP* auch global vorgenommen werden. Deshalb werden hier nur eine Liste der Einstellungsmöglichkeiten und die Unterschiede zu den globalen Einstellungen aufgeführt.

   Die folgenden Einstellungen können vorgenommen werden:

   - **Routing:** Auf der Registerkarte *Routing* können Sie Domänen- und Routingziele für den SMTP-Proxy konfigurieren. Außerdem können Sie festlegen, wie Empfänger verifiziert werden sollen.
     - Statische Hostliste
     - DNS-Hostname
     - MX-Einträge

     Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Routing*.

   - **Empfängerverifizierung**
     Empfänger verifizieren: Hier können Sie festlegen, ob und wie E-Mail-Empfänger verifiziert werden.

     - **Mit Serveranfrage:** Es wird eine Anfrage an den Server geschickt, um den Empfänger zu verifizieren.

- **Im Active Directory:** Es wird eine Anfrage an den Active-Directory-Server geschickt, um den Empfänger zu verifizieren. Um Active Directory benutzen zu können, muss ein Active-Directory-Server unter *Definitionen & Benutzer > Authentifizierungsdienste > Server* angegeben worden sein. Geben Sie einen BaseDN im Feld *Alternativer BaseDN* ein.

  Hinweis – Die Verwendung der Active-Directory-Empfängerverifizierung kann dazu führen, dass Nachrichten abgelehnt werden, wenn der Server nicht antwortet.

- **Aus:** Sie können die Empfängerverifizierung vollständig ausschalten, aber das ist nicht empfehlenswert, da es zu einem höheren Spam-Aufkommen und Wörterbuchangriffen führt. Dadurch erhöhen Sie die Wahrscheinlichkeit, dass Ihre Quarantäne mit unerwünschten Nachrichten „überflutet" wird.

Weitere Informationen finden Sie unter *Email Protection > SMTP > Routing*.

- **Sophos UTM RBLs:** Hier können Sie IP-Adressen blockieren, die mit Spamversand in Verbindung gebracht werden.
  - Empfohlene RBLs verwenden

  Weitere Informationen finden Sie unter *Email Protection > SMTP > Antispam*.

- **Extra-RBLs:** Sie können zusätzliche RBL-Sites hinzufügen, um die Antispam-Fähigkeiten von Sophos UTM zu erweitern. Weitere Informationen finden Sie unter *Email Protection > SMTP > Antispam*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **BATV/RDNS/HELO/SPF/Greylisting:** Auf dieser Registerkarte sind verschiedene erweiterte Optionen vereint, die die Antispam-Fähigkeiten von Sophos UTM ergänzen.
  - Ungültige HELO/fehlende RDNS ablehnen
  - Greylisting verwenden
  - BATV verwenden
  - SPF-Prüfung durchführen

  Weitere Informationen finden Sie unter *Email Protection > SMTP > Antispam*.

- **Antiviren-Scan:** Hier können Sie festlegen, wie mit Nachrichten verfahren wird, die schädlichen Inhalt besitzen. Die folgenden Aktionen sind möglich:
  - Aus
  - Quarantäne
  - Verwerfen

  Sie können zwischen den folgenden Antiviren-Scan-Optionen wählen:

  - **Einzelscan:** Standardeinstellung; bietet maximale Leistung. Die auf der Registerkarte *Systemeinstellungen* > *Scan-Einstellungen* festgelegte Engine wird verwendet.
  - **Zweifachscan:** Bietet maximale Erkennungsrate, da der entsprechende Verkehr von zwei verschiedenen Virenscannern gescannt wird. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist.

  Unscannbaren und verschlüsselten Inhalt in Quarantäne: Wählen Sie diese Option, um E-Mails unter Quarantäne zu stellen, deren Inhalt nicht gescannt werden konnte. Unscannbarer Inhalt können verschlüsselte Archive oder sehr große Inhalte sein, oder es kann ein technischer Grund vorliegen wie z. B. der Ausfall eines Scanners.

  Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antivirus*.

- **Antispam-Scan:** Hier können Sie konfigurieren, wie mit unerwünschten kommerziellen E-Mails verfahren werden soll.Sowohl für Spam als auch für bestätigten Spam können Sie zwischen den folgenden Optionen wählen:
  - Aus
  - Warnen
  - Quarantäne
  - Verwerfen

  Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antispam*.

- **Absender-Blacklist:** Der Envelope-Absender eingehender SMTP-Sitzungen wird mit den Adressen auf dieser Blacklist (Negativliste) verglichen. Wenn der Envelope-Absender auf der Blacklist gefunden wird, wird die Nachricht verworfen. Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antispam*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **MIME Audio/Video/Exe-Datei-Blockierung:** Der MIME-Typ-Filter liest den Typ von E-Mail-Inhalten aus.Sie können wählen, welche Inhaltsarten Sie unter Quarantäne stellen wollen:
  - Audioinhalte
  - Videoinhalte
  - Ausführbare Inhalte

  Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antivirus*.

- **MIME-Typ-Blacklist:** Hier können Sie zusätzliche MIME-Typen hinzufügen, die unter Quarantäne gestellt werden sollen. Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antivirus*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **MIME-Typ-Whitelist:** Hier können Sie MIME-Typen hinzufügen, die nicht unter Quarantäne gestellt werden sollen. Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antivirus*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **Blockierte Erweiterungen:** Mit dem *Dateierweiterungenfilter* können Sie E-Mails unter Quarantäne stellen (mit Warnung), die bestimmte Dateitypen enthalten, basierend auf ihren Dateierweiterungen (z. B. ausführbare Dateien).Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antivirus*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **Blockierte Ausdrücke:** Der Ausdruckfilter prüft den Inhalt von Nachrichten, die den SMTP-Proxy passieren, auf bestimmte Ausdrücke. Verdächtige E-Mails werden blockiert. Weitere Informationen finden Sie unter *Email Protection* > *SMTP* > *Antispam*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **Vertraulichkeitsfußzeile:** Sie können jeder ausgehenden E-Mail eine Vertraulichkeitsfußzeile hinzufügen, die Benutzer zum Beispiel darüber informiert, dass die E-Mail vertrauliche oder schutzwürdige Informationen enthalten kann, und sie anpassen. Die Vertraulichkeitsfußzeile wird jedoch nicht an die E-Mail angehängt, wenn es sich bei der E-Mail um eine Antwort handelt (d. h. sie besitzt den Header *In-Reply-To*) oder wenn die Inhaltsart der E-Mail nicht bestimmt werden konnte. Beachten Sie, dass die Fußzeile abhängig von der Absenderdomäne

angehängt wird. Um eine Fußzeile zu verwenden, markieren Sie das Auswahlkästchen und geben Sie den Text für die Fußzeile ein.

- **SPX-Vorlagenauswahl:** Die SPX-Vorlage wird für SPX-Verschlüsselung verwendet. Sie definiert, wie verschlüsselte E-Mails an die Empfänger versendet werden. Weitere Informationen finden Sie unter *Email Protection > SPX-Verschlüsselung > SPX-Vorlagen*.
- **Konfiguration von Data Protection:** Hier können Sie Anhänge zur Scanliste hinzufügen, Benachrichtigungen festlegen und die Elemente der *SophosLabs-Inhaltssteuerungslisten* auswählen.
  Weitere Informationen finden Sie unter *SMTP > Data Protection*.

6. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.Das neue Profil wird in der Liste *SMTP-Profile* angezeigt.

Hinweis – Wenn Sie die Option *Globale Einstellungen verwenden* für eine Einstellung verwenden und auf *Übernehmen* klicken, wechselt das Symbol der Funktion zum Symbol für globale Einstellungen. Dadurch erhalten Sie leicht einen Überblick darüber, für welche Funktionen Sie die globalen Einstellungen verwenden und für welche Funktionen die individuellen Einstellungen.

Um ein Profil umzubenennen, zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen oben unter der Auswahlliste der Profile.

10.3 POP3

Im Menü *Email Protection > POP3* können Sie den POP3-Proxy für eingehende E-Mails konfigurieren. Das *Post Office Protocol 3* ist ein Internet-Standardprotokoll auf Anwendungsebene, das es ermöglicht, E-Mails von einem entfernten Server abzuholen. Der POP3-Proxy arbeitet im Transparenzmodus, das heißt, alle POP3-Anfragen, die über Port `110` (und`995`, wenn das Scannen von TLS-verschlüsseltem Verkehr aktiviert ist) aus dem internen Netzwerk kommen, werden abgefangen und, unsichtbar für den Client, durch den Proxy geleitet. Der Vorteil dieses Modus ist, dass keine zusätzliche Verwaltung oder clientseitige Konfiguration nötig ist.

Hinweis – Es kann nötig sein, die Einstellungen für die Server-Zeitüberschreitung in der E-Mail-Client-Konfiguration zu erhöhen. Meistens ist die Voreinstellung von einer Minute oder weniger zu gering, insbesondere wenn große E-Mails abgeholt werden.

Das POP3-Protokoll verfolgt auf der Serverseite nicht, welche E-Mails bereits abgeholt wurden. Im Allgemeinen holt ein Mail-Client eine E-Mail ab und löscht sie danach auf dem Server. Wenn der Client jedoch so eingestellt ist, dass er keine E-Mails löscht, dann wird auch auf Serverseite nicht gelöscht und der Client übernimmt die Aufgabe, nachzuvollziehen, welche E-Mails bereits abgeholt wurden.

10.3.1 Allgemein

Auf der Registerkarte *Email Protection* > *POP3* > *Allgemein* können Sie Grundeinstellungen für den POP3-Proxy vornehmen.

Um den POP3-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den POP3-Proxy.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *POP3-Einstellungen* kann bearbeitet werden.

2. **Wählen Sie die zugelassenen Netzwerke aus.**
   Fügen Sie die Netzwerke hinzu oder wählen Sie die Netzwerke aus, deren POP3-Verkehr über den Proxy laufen soll. Standardmäßig ist das interne Netzwerk (Internal Network) voreingestellt. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   Warnung – Wählen Sie niemals das Netzwerkobjekt *Any* aus, weil Sie dadurch Ihre Appliance einem hohen Risiko für Angriffe aus dem Internet aussetzen würden.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

Live-Protokoll

Im *POP3-Live-Protokoll* werden die Aktivitäten des POP3-Proxy protokolliert. Alle eingehenden E-Mails werden darin aufgeführt. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

10.3.2 Antivirus

Die Registerkarte *Antivirus* bietet verschiedene Maßnahmen gegen E-Mails, die schädlichen oder gefährlichen Inhalt haben wie Viren, Würmer oder andere Schadsoftware.

Antiviren-Scan

Wenn Sie diese Option wählen, werden E-Mails nach unerwünschtem Inhalt gescannt wie z. B. Viren, Trojanischen Pferden oder verdächtigen Dateitypen. Nachrichten mit schädlichem Inhalt werden blockiert oder in der E-Mail-Quarantäne gespeichert. Benutzer können ihre unter Quarantäne stehenden E-Mails ansehen und freigeben, entweder über das SophosBenutzerportal oder den täglichen Quarantänebericht. Nachrichten, die schädlichen Inhalt enthalten, können jedoch nur vom Administrator über den Mail-Manager aus der Quarantäne freigegeben werden.

Sophos UTMbietet mehrere Antiviren-Mechanismen für höchste Sicherheit.

- **Einzelscan:** Standardeinstellung; bietet maximale Leistung. Die auf der Registerkarte *Systemeinstellungen* > *Scan-Einstellungen* festgelegte Engine wird verwendet.
- **Zweifachscan:** Bietet maximale Erkennungsrate, da der entsprechende Verkehr von zwei verschiedenen Virenscannern gescannt wird. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist.

Unscannbaren und verschlüsselten Inhalt in Quarantäne: Wählen Sie diese Option, um E-Mails unter Quarantäne zu stellen, deren Inhalt nicht gescannt werden konnte. Unscannbarer Inhalt können verschlüsselte Archive oder sehr große Inhalte sein, oder es kann ein technischer Grund vorliegen wie z. B. der Ausfall eines Scanners.

Max. Scangröße: Legen Sie die Maximalgröße von Dateien fest, die von den Antiviren-Engines gescannt werden sollen. Dateien, die größer sind, werden nicht gescannt.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Dateierweiterungenfilter

Mit dieser Funktion können Sie E-Mails unter Quarantäne stellen (mit Warnung), die bestimmte Dateitypen enthalten, basierend auf ihren Dateierweiterungen (z. B. ausführbare Dateien).
Um Dateierweiterungen hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Blockierte Erweiterungen* und geben Sie eine kritische Dateierweiterung ein, die gesperrt werden soll, z. B. `exe` oder `jar` (ohne den Punkt als Trennzeichen). Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Archive können nicht auf verbotene Dateierweiterungen gescannt werden. Um Ihr Netzwerk vor Schadsoftware aus Archivdateien zu schützen, sollten Sie in Betracht ziehen, die entsprechenden Archivdateierweiterungen gänzlich zu blockieren.

10.3.3 Antispam

Sophos UTMkann so konfiguriert werden, dass es unerwünschte Spam-E-Mails entdeckt und Spam-Übermittlungen von bekannten oder verdächtigten Spam-Versendern identifiziert. Die Konfigurationsoptionen auf der Registerkarte *Antispam* ermöglichen die Konfiguration von POP3-Sicherheitsfunktionen, die darauf ausgelegt sind, Ihr Netzwerk vor dem Empfang von unerbetenen kommerziellen E-Mails zu schützen.

Spamfilter

Sophos UTMbietet eine heuristische Prüfung eingehender E-Mails auf Spam-Eigenschaften. Sie benutzt dafür SMTP-Envelope-Informationen (envelope = Umschlag) und eine interne Datenbank mit heuristischen Tests und Eigenschaften. Die Spamfilter-Option bewertet Nachrichten basierend auf ihrem Inhalt und SMTP-Envelope-Informationen. Höhere Werte deuten auf eine höhere Spam-Wahrscheinlichkeit hin.

Mit den folgenden beiden Optionen können Sie festlegen, was mit Nachrichten geschehen soll, denen ein gewisser Spam-Wert zugewiesen wurde. So wird sichergestellt, dass potenzielle Spam-E-Mails vom Gateway anders behandelt werden.

- **Spam-Aktion:** Hier können Sie festlegen, was mit Nachrichten geschieht, die als möglicher Spam eingestuft wurden.
- **Aktion bei bestätigtem Spam:** Hier können Sie festlegen, was mit Nachrichten geschieht, die sicher Spam sind.

Sie können zwischen verschiedenen Aktionen für diese beiden Arten von Spam wählen:

- **Aus:** Es werden keine Nachrichten als Spam markiert oder ausgefiltert.
- **Warnen:** Es werden keine Nachrichten herausgefiltert. Stattdessen wird eine Spam-Markierung („Flag") zum Header der Nachricht hinzugefügt und der Betreff der Nachricht erhält eine Spam-Kennzeichnung.
- **Quarantäne:** Die Nachricht wird blockiert und in die E-Mail-Quarantäne verschoben. Nachrichten in Quarantäne können entweder über das Benutzerportal oder den täglichen Quarantänebericht eingesehen werden.

Spam-Kennzeichnung: Mit dieser Option können Sie eine Kennzeichnung für Spam-Nachrichten festlegen, d. h., dass eine Zeichenkette zur Betreffzeile der Nachricht hinzugefügt wird, die es einfach macht, Spam-Nachrichten schnell als solche zu erkennen. Standardmäßig wird die Zeichenkette `*SPAM*` benutzt, um Nachrichten als Spam zu kennzeichnen.

Ausdruckfilter

Der Ausdruckfilter scannt den Betreff und Inhalt von Nachrichten auf spezifische Ausdrücke. E-Mails, die einen der hier aufgeführten Ausdrücke enthalten, werden blockiert. Wenn jedoch auf der Registerkarte *Email Protection* > *POP3* > *Erweitert* die Vorabholung eingeschaltet ist, wird die E-Mail unter Quarantäne gestellt. Ausdrücke können in Form von *Perl Compatible Regular Expressions* (Perl-kompatiblen regulären Ausdrücken) eingegeben werden. Einfache Zeichenfolgen wie „Online Dating" werden ohne Berücksichtigung der Groß-/Kleinschreibung interpretiert.

Querverweis – Detaillierte Informationen zur Verwendung von regulären Ausdrücken im Ausdruckfilter finden Sie in der Sophos-Knowledgebase.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Absender-Blacklist

Der Envelope-Absender eingehender POP3-Sitzungen wird mit den Adressen auf dieser Blacklist (Negativliste) verglichen. Wenn der Envelope-Sender auf der Blacklist gefunden wird, wird die Nachricht unter Quarantäne gestellt und mit *Other* in der Betreffzeile markiert.
Um ein neues Adress-Pattern zur Blacklist hinzuzufügen, klicken Sie auf das Plussymbol im Feld *Adress-Patterns auf Blacklist*, geben Sie eine (oder einen Teil einer) Adresse ein und klicken Sie auf *Übernehmen*. Sie können einen Asterisk (*) als Platzhalter verwenden, z. B. `*@abbeybnknational.com`.

Tipp – Endbenutzer können im Benutzerportal ihre eigenen Black- und Whitelisten anlegen.

10.3.4 Ausnahmen

Auf der Registerkarte *POP3 > Ausnahmen* können Sie Clienthosts/-Netzwerke und Absenderadressen festlegen, die von verschiedenen Sicherheitsmaßnahmen ausgenommen werden sollen.

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahmenliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Ausnahme ein.

   Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, die nicht durchgeführt werden sollen. Weitere Informationen finden Sie unter *Email Protection > POP3 > Antivirus* und *Antispam*.

   Für diese Clienthosts/-Netzwerke: Fügen Sie die Quellhosts/-Netzwerke (d. h. die Hosts oder Netzwerke, die Nachrichten senden) hinzu bzw. wählen Sie die Quellhosts/-Netzwerke aus, die von den Sicherheitsprüfungen ausgenommen werden sollen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Hinweis – Für Localhost muss keine Ausnahmeregel angelegt werden, da lokale Nachrichten standardmäßig nicht gescannt werden.

   Wenn Sie diese Option wählen, wird das Feld *Clienthosts/-netzwerke* geöffnet. Hier können Sie einen Host oder ein Netzwerk eingeben, indem Sie auf das Plussymbol oder das Ordnersymbol klicken.

   ODER Diese Empfängeradressen: Wählen Sie die Absenderadressen, die von den gewählten Sicherheitsprüfungen ausgenommen werden sollen.
   Wenn Sie diese Option wählen, wird das Feld *Absender* geöffnet. Sie können entweder eine vollständige, gültige E-Mail-Adresse eingeben (z. B. `mmustermann@beispiel.de`) oder alle E-Mail-Adressen einer bestimmten Domäne, wobei Sie einen Asterisk (*) als Platzhalter verwenden (z. B. `*@beispiel.de`).

> **Hinweis –** Verwenden Sie die *Absender*-Option mit Vorsicht, da Absenderadressen leicht gefälscht werden können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

10.3.5 Erweitert

Auf der Registerkarte *POP3* > *Erweitert* können Sie Hosts und Netzwerke bestimmen, die vom Transparenzmodus des POP3-Proxy ausgenommen sein sollen. Des Weiteren beinhaltet die Registerkarte die POP3-Option zum Vorabholen (engl. prefetch), welche es ermöglicht, Nachrichten von einem POP3-Server im Voraus zu holen und sie in einer Datenbank zu speichern.

Transparenzmodus-Ausnahmen

Hosts und Netzwerke, die im Feld *Auszunehmende Hosts/Netze* aufgeführt sind, werden vom POP3-Proxy nicht transparent überwacht. Um jedoch POP3-Verkehr für diese Hosts und Netzwerke zuzulassen, wählen Sie die Option *POP3-Verkehr für aufgeführte Hosts/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezielle Firewallregeln für die hier aufgeführten Hosts und Netzwerke anlegen.

POP3-Server und Vorabholen

Sie können hier einen oder mehrere POP3-Server eintragen, die in Ihrem Netzwerk oder von Ihren Endbenutzern verwendet werden und dem Proxy bekannt sein sollen. Zusätzlich können Sie das Vorabholen (engl. prefetching) aktivieren.

Um einen POP3-Server anzulegen, gehen Sie folgendermaßen vor:

1. **Geben Sie den DNS-Namen des oder der POP3-Server ein.**
   Klicken Sie im Feld *POP3-Server* auf das Plussymbol.Geben Sie im Dialogfenster *Server hinzufügen* den DNS-Namen ein und klicken Sie auf *Speichern*.

Ein neuer Eintrag mit dem DNS-Namen und dem Zusatz *Servers* wird im Feld angezeigt. Die UTM legt automatisch eine DNS-Gruppe mit dem festgelegten DNS-Namen an und verknüpft ihn mit dem neuen POP3-Server-Eintrag.

2. **Legen Sie die Eigenschaften des POP3-Servers fest.**
   Klicken Sie im Feld *POP3-Server* auf das Bearbeiten-Symbol vor dem POP3-Server. Das Dialogfenster *Server bearbeiten* wird geöffnet. Nehmen Sie die folgenden Einstellungen vor:

   Name: Ändern Sie bei Bedarf den Namen des POP3-Servers.

   Hosts: Das Feld enthält automatisch eine DNS-Gruppe mit dem oben festgelegten DNS-Namen. Fügen Sie zusätzliche Hosts oder DNS-Gruppen hinzu oder wählen Sie sie aus. Stellen Sie sicher, dass Sie nur Hosts und DNS-Gruppen hinzufügen, die dieselben POP3-Accounts bedienen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   TLS-Zertifikat: Wählen Sie aus der Auswahlliste ein Zertifikat zum Aushandeln der TLS-Verschlüsselung mit allen Gegenstellen aus, die TLS unterstützen. Auf der Registerkarte *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Zertifikate* können Sie Zertifikate erstellen oder hochladen.

   Hinweis – Damit die TLS-Verschlüsselung funktioniert, muss die Option *TLS-verschlüsselten POP3-Verkehr scannen* im Bereich *TLS-Einstellungen* aktiviert werden. Für POP3-Server, die hier nicht festgelegt sind oder die kein TLS-Zertifikat besitzen, können Sie im Bereich *TLS-Einstellungen* ein Standard-TLS-Zertifikat festlegen.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Der POP3-Server ist angelegt.

Wenn kein POP3-Server angegeben wird und E-Mails vom Proxy abgefangen werden, ersetzt der Proxy die E-Mails sofort mit einer Benachrichtigung an den Empfänger, die ihn davon in Kenntnis setzt, dass die E-Mails unter Quarantäne gestellt wurden. E-Mails in Quarantäne können im *Mail-Manager* eingesehen werden, aber da sie nicht mit einem Server oder einem Konto in Verbindung gebracht werden können, können sie bei einer späteren Verbindung nicht freigegeben werden. Die Freigabe von E-Mails ist überhaupt nur möglich für E-Mails, die im Voraus abgeholt wurden („prefetching“).

Es gibt zwei Szenarien:

- Wenn ein oder mehrere POP3-Server angegeben sind und Vorabholen deaktiviert ist, behält der Proxy die Übersicht darüber, welche E-Mails in Quarantäne zu welchem Server oder Konto gehören. Dadurch können E-Mails in Quarantäne freigegeben werden, wenn der Client die Mailbox das nächste Mal abfragt. Damit das funktioniert, muss der Proxy sicher feststellen, welche IP-Adresse zu welchem Server gehört (über deren FQDN, die Sie in Ihrem Mail-Client angegeben haben).
- Wenn ein oder mehrere POP3-Server angegeben sind und Vorabholen aktiviert ist, überprüft der POP3-Proxy die POP3-Server periodisch auf neue Nachrichten. Wenn eine neue Nachricht angekommen ist, wird sie zum POP3-Proxy kopiert, gescannt und in einer Datenbank auf der UTM gespeichert. Die Nachricht bleibt auf dem POP3-Server. Wenn ein Client versucht, neue Nachrichten abzuholen, kommuniziert er stattdessen mit dem POP3-Proxy und holt nur die Nachrichten aus der Datenbank.

Ein POP3-Proxy, der das Vorabholen unterstützt, hat unter anderem folgende Vorteile:

- Keine Zeitüberschreitungsprobleme zwischen Client und Proxy oder umgekehrt.
- Die Zustellung der Nachrichten erfolgt sehr viel schneller, da die E-Mails bereits vorab gescannt wurden.
- Blockierte Nachrichten können vom Benutzerportal aus freigegeben werden – sie werden beim nächsten Abrufen der E-Mails mit abgeholt.

Wenn eine Nachricht blockiert wurde, weil sie schädlichen Inhalt enthält oder als Spam eingestuft wurde, wird sie nicht an den Client ausgeliefert. Stattdessen wird sie unter Quarantäne gestellt. Eine Nachricht, die unter Quarantäne gestellt ist, wird im Bereich *Mail-Manager* im Benutzerportal gespeichert, von wo sie gelöscht oder freigegeben werden kann.

Vorabholen verwenden: Um den Vorabholenmodus zu aktivieren, markieren Sie das Auswahlkästchen und fügen Sie einen oder mehrere POP3-Server zum Feld *POP3-Server* hinzu.

> **Vorabholenintervall:** Wählen Sie das Zeitintervall, in dem der POP3-Proxy den POP3-Server kontaktiert, um Nachrichten vorab zu holen.
>
> **Hinweis –** Das Intervall, in dem Mail-Clients den POP3-Server kontaktieren dürfen, variiert von Server zu Server. Das Vorabholenintervall sollte deshalb nicht kürzer eingestellt werden als der POP3-Server es zulässt, sonst schlägt das Herunterladen der POP3-Nachrichten fehl, da der Zugang zum POP3-Server nicht gestattet ist. Beachten Sie auch, dass mehrere Clients das gleiche POP3-Konto abfragen können. Jedes Mal, wenn Nachrichten erfolgreich vom POP3-Server abgerufen wurden,

beginnt die Zeiterfassung von vorne, bis eine erneute Abfrage möglich ist. Wenn aus diesem Grund der POP3-Proxy den POP3-Server viermal hintereinander nicht erreichen kann (Standardeinstellung ist alle 15 Minuten), wird das Kontokennwort aus der Proxy-Mail-Datenbank gelöscht, und es werden dann solange keine E-Mails mehr abgeholt, bis ein Mail-Client das Kennwort an den POP3-Server schickt und sich wieder erfolgreich anmeldet.

Quarantäne-Nachrichten vom Server löschen: Wenn Sie diese Option wählen, werden Nachrichten in Quarantäne sofort vom POP3-Server gelöscht. Das ist nützlich, um zu verhindern, dass Benutzer Spam- oder mit Viren infizierte Nachrichten erhalten, wenn sie sich mit dem POP3-Server nicht über die UTM, sondern beispielsweise über das Webportal des POP3-Servers verbinden.

Wenn der E-Mail-Client so konfiguriert ist, dass er Nachrichten vom Server löscht, nachdem er sie abgeholt hat, wird diese Information auch in der Datenbank abgespeichert. Das nächste Mal, wenn der Proxy Nachrichten für dieses POP3-Konto vorab holt, wird er die Nachrichten vom Server löschen. Das bedeutet, so lange kein Client Nachrichten von Sophos UTM abruft *und* kein Löschbefehl konfiguriert ist, werden keine Nachrichten auf dem POP3-Server gelöscht. Dadurch können sie weiterhin gelesen werden, zum Beispiel über das Webportal des E-Mail-Anbieters.
Quarantäne-Nachrichten werden in folgenden Fällen vom POP3-Server gelöscht:

- Die Nachrichten werden manuell über den Mail-Manager gelöscht.
- Die Nachrichten werden manuell über das Benutzerportal gelöscht.
- Die Nachricht wurde freigegeben (entweder über den Quarantänebericht oder das Benutzerportal) und der E-Mail-Client des Benutzers ist so konfiguriert, dass er Nachrichten nach der Zustellung löscht.
- Die Benachrichtigungs-E-Mail wurde gelöscht.
- Die Aufbewahrungsfrist ist abgelaufen (siehe Abschnitt *Konfiguration* im Kapitel *Mail-Manager*).

Im Vorabholenmodus können Nachrichten unter Quarantäne nicht direkt durch einen Client-Befehl vom POP3-Server gelöscht werden.

Hinweis – Der E-Mail-Client muss sich mindestens einmal erfolgreich mit dem POP3-Server verbunden haben, bevor das Vorabholen funktioniert. Das liegt daran, dass Sophos UTM

den Namen des POP3-Servers, den Benutzernamen und das Benutzerkennwort in einer Datenbank speichern muss, um POP3-Nachrichten anstelle des Benutzers abholen zu können. Das kann jedoch *nicht* dadurch erreicht werden, dass die POP3-Kontozugangsdaten im Sophos Benutzerportal eingerichtet werden. Die POP3-Kontozugangsdaten im Benutzerportal werden benötigt, damit die vorab geholten Nachrichten im Benutzerportal und im täglichen Quarantänebericht des entsprechenden Benutzers erscheinen.

Hinweis für Benutzer von Fetchmail: Die `TOP`-Methode wird aus Sicherheitsgründen nicht unterstützt, um E-Mails vom Mailserver herunterzuladen – Nachrichten, die über `TOP` empfangen wurden, können nicht gescannt werden. Es funktioniert aber, wenn Sie die Option `fetchall` angeben (`-a` auf der Kommandozeile). Um weitere Informationen zu erhalten, lesen Sie bitte das Kapitel „RETR or TOP“ im Fetchmail-Handbuch.

Bevorzugter Zeichensatz

In diesem Abschnitt können Sie einen anderen Zeichensatz als UTF-8 wählen, der für jene Mail-Header verwendet werden soll, die irgendwie von der UTM verändert wurden (z. B. durch BATV). Das ist nützlich, wenn Ihre Benutzer Mail-Clients verwenden, die mit UTF-8 nicht umgehen können. Im Allgemeinen ist der voreingestellte Zeichensatz eine gute Wahl, unabhängig von Ihrer Region. Deshalb sollten Sie diese Einstellung nur ändern, wenn Sie sicher sind, dass es das ist, was Sie wollen.Wenn Sie Zweifel haben, sollten Sie *UTF-8* beibehalten.

TLS-Einstellungen

TLS-verschlüsselten POP3-Verkehr scannen: Wenn diese Option aktiviert ist, scannt die UTM TLS-verschlüsselten POP3-Verkehr. Damit dies funktioniert, müssen TLS-Zertifikate für die POP3-Server, auf die die POP3-Clients zugreifen, definiert werden (siehe Abschnitt *POP3-Server und Vorabholen* oben und Option *TLS-Zertifikat* unten).

Wenn die Option deaktiviert ist und ein POP3-Client versucht, über TLS auf einen POP3-Server zuzugreifen, wird die Verbindung nicht hergestellt.

TLS-Zertifikat: Wählen Sie ein Zertifikat aus der Auswahlliste. Dieses wird verwendet für die TLS-Verschlüsselung mit allen POP3-Clients, die TLS unterstützen und versuchen, auf einen POP3-Server zuzugreifen, der entweder nicht im Feld *POP3-Server* oben enthalten ist oder kein passendes TLS-Zertifikat besitzt. Das gewählte Zertifikat wird dem POP3-Client angeboten. POP3-Clients verifizieren normalerweise, dass das vom POP3-Server angebotene TLS-Zertifikat mit dem konfigurierten POP3-Servernamen übereinstimmt. Aus diesem Grund werden die meisten POP3-Clients eine Warnung ausgeben, dass der Hostname

des Zertifikats nicht mit dem erwarteten konfigurierten POP3-Servernamen übereinstimmt. Der Benutzer kann diese Warnung jedoch ignorieren und sich trotzdem verbinden. Um diese Warnung zu verhindern müssen Sie alle verwendeten *POP3-Server* in das Feld POP3-Server oben eingeben und für jeden der Server ein passendes TLS-Zertifikat konfigurieren.

Wenn hier kein Zertifikat ausgewählt ist und ein POP3-Client versucht, über TLS einen POP3-Server zu erreichen, der nicht im Feld *POP3-Server* enthalten ist oder kein passendes TLS-Zertifikat besitzt, wird die Verbindung nicht aufgebaut.

Tipp –Auf der Registerkarte *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Zertifikate* können Sie Zertifikate erstellen oder hochladen.

10.4 Email Encryption

Seitdem E-Mails im privaten und geschäftlichen Bereich das primäre elektronische Kommunikationsmittel geworden sind, sind verständliche Bedenken über Privatsphäre und Authentifizierung aufgekommen. Einfach formuliert: Das E-Mail-Format wird in Klartext übermittelt, ähnlich einer Postkarte, die jeder lesen kann. Da es darüber hinaus sehr einfach ist, falsche Identitäten anzunehmen, muss der Empfänger feststellen können, ob der Absender auch der ist, für den er sich ausgibt.

Die Lösung dieser Probleme ist typischerweise die Verwendung von E-Mail-Verschlüsselung und digitalen Zertifikaten – E-Mails werden dabei elektronisch signiert und kryptografisch verschlüsselt. Dies stellt sicher, dass ausschließlich der Nachrichtenempfänger diese öffnen, den Inhalt der Nachricht anzeigen (Privatsphäre) und die Identität des Absenders feststellen kann (Authentifizierung). Anders ausgedrückt: Dieser Prozess vereitelt die Idee, eine „E-Postkarte“ zugeschickt zu bekommen, und führt einen Prozess ein, der registrierten oder zertifizierten E-Mails ähnelt.

In der modernen Kryptografie gibt es zwei Verfahren für die Verschlüsselung von E-Mails: symmetrische und asymmetrische. Beide Verfahren haben sich als Standards etabliert und werden in verschiedenen Anwendungen eingesetzt. Bei der symmetrischen Verschlüsselung teilen sich Absender und Empfänger den gleichen Schlüssel.

Bei der asymmetrischen Verschlüsselung hingegen (auch bekannt als Public-Key-Kryptografie) besitzt jeder Benutzer ein Schlüsselpaar – einen öffentlichen Schlüssel (Public Key) für die Verschlüsselung der E-Mail und einen korrespondierenden privaten bzw. geheimen Schlüs-

sel (Private Key) zur Entschlüsselung. Der öffentliche Schlüssel wird frei verteilt, während der private Schlüssel vom Benutzer geheim gehalten wird.

Ein Nachteil der symmetrischen Verschlüsselung ist, dass sich die beiden Beteiligten für eine sichere Kommunikation über den Schlüssel abstimmen und sicherstellen müssen, dass nur ihnen der Schlüssel bekannt ist. Wenn sie sich an unterschiedlichen Standorten befinden, müssen sie sicherstellen, dass der Schlüssel bei der Übermittlung geheim bleibt. Das größte Problem bei der symmetrischen Verschlüsselung ist daher die Übermittlung der Schlüssel: Wie sende ich den Schlüssel an den Empfänger, ohne dass ihn jemand abfängt? Die Public-Key-Kryptografie wurde entwickelt, um genau diese Sicherheitslücke zu schließen. Mit dieser Verschlüsselungsmethode können zwei Parteien über eine unsichere Verbindung auf sichere Weise miteinander kommunizieren, ohne dass zuvor ein gemeinsamer Schlüssel festgelegt werden muss.

Der Bedarf an E-Mail-Verschlüsselung hat eine Reihe von Standards für die Public-Key-Kryptografie hervorgebracht, vor allem S/MIME und OpenPGP. Sophos UTM unterstützt beide Standards. S/MIME (*Secure Multipurpose Internet Mail Extensions*) ist ein Standard für asymmetrische Verschlüsselung und das Signieren von MIME-strukturierten E-Mails. Dieses Protokoll wird üblicherweise innerhalb einer Public-Key-Infrastruktur (PKI) eingesetzt und basiert auf einer hierarchischen Struktur aus digitalen Zertifikaten, wobei es eine vertrauenswürdige Instanz als Zertifizierungsstelle (CA) benötigt. Die CA stellt ein Zertifikat aus, bei dem sie eine Identität an ein Paar elektronischer Schlüssel bindet. Dieser Vorgang kann als digitales Gegenstück zu herkömmlichen Identitätsdokumenten wie einem Reisepass angesehen werden. Aus technischer Sicht stellt die CA ein Zertifikat aus, indem sie einen öffentlichen Schlüssel an einen bestimmten *Distinguished Name* im X.500-Standard oder an einen *Alternative Name* wie z. B. eine E-Mail-Adresse bindet.

Ein digitales Zertifikat ermöglicht es festzustellen, ob jemand die Berechtigung hat, einen angegebenen Schlüssel zu verwenden. Der Gedanke dahinter ist, dass man sicher sein kann, dass jemandem der fragliche öffentliche Schlüssel gehört, wenn dieser einer CA vertraut und nachweisen kann, dass der öffentliche Schlüssel von dieser CA signiert wurde.

OpenPGP (*Pretty Good Privacy*), der andere Standard, nutzt eine asymmetrische Verschlüsselung, die üblicherweise in einem sogenannten *Web of Trust* (WOT, „Netz des Vertrauens“) eingesetzt wird. Das bedeutet, dass öffentliche Schlüssel digital von anderen Benutzern signiert werden, welche durch diese Handlung die Zusammengehörigkeit von Schlüssel und Benutzer bestätigen.

Hinweis – Beachten Sie, dass die beiden Standards S/MIME und OpenPGP, obwohl sie ähnliche Dienste anbieten, sehr unterschiedliche Formate aufweisen. Das bedeutet, dass Benutzer des einen Protokolls nicht mit Benutzern des anderen Protokolls kommunizieren können. Des Weiteren können Authentifizierungszertifikate nicht für beide Protokolle verwendet werden.

Die gesamte E-Mail-Verschlüsselung ist für den Benutzer transparent, sodass keine zusätzliche Verschlüsselungs-Software auf dem Client installiert werden muss. Einfach gesagt heißt das, dass zur Verschlüsselung der E-Mails das Zertifikat der Zielpartei oder der öffentliche Schlüssel benötigt wird. Nachfolgend sind die unterschiedlichen Funktionsweisen für ein- und ausgehende Nachrichten beschrieben:

- Ausgehende Nachrichten von internen Benutzern werden standardmäßig gescannt, automatisch signiert und verschlüsselt. Für die Signierung und die Verschlüsselung wird entweder das Zertifikat (S/MIME) oder der öffentliche Schlüssel (OpenPGP) des Empfängers verwendet. Das Zertifikat oder der öffentliche Schlüssel müssen dafür auf UTM vorhanden sein.
- Verschlüsselte eingehende Nachrichten von externen Benutzern, deren S/MIME-Zertifikat oder öffentlicher OpenPGP-Schlüssel UTM bekannt ist, werden automatisch entschlüsselt und auf Viren überprüft.Um die Nachricht zu entschlüsseln, muss der S/MIME-Schlüssel oder der private OpenPGP-Schlüssel des internen Benutzers auf UTM installiert sein.
- Verschlüsselte eingehende Nachrichten von externen Benutzern oder für interne, der UTM unbekannte Benutzer werden zugestellt, obwohl sie nicht entschlüsselt und deshalb nicht auf Viren oder Spam gescannt werden können. Es liegt dann in der Verantwortung des Empfängers (interner Benutzer), sicherzustellen, dass die E-Mail keine Schadsoftware enthält, beispielsweise durch die Benutzung einer eigenen Firewall.
- Ausgehende Nachrichten, die bereits clientseitig verschlüsselt wurden, werden direkt an den Empfänger weitergeleitet, wenn das entsprechende Zertifikat (S/MIME) oder der öffentliche Schlüssel (OpenPGP) nicht bekannt ist. Falls jedoch das S/MIME-Zertifikat oder der öffentliche OpenPGP-Schlüssel des Empfängers vorhanden ist, werden die Nachrichten ein zweites Mal verschlüsselt. Beachten Sie, dass im Voraus verschlüsselte Nachrichten nicht auf schädlichen Inhalt gescannt werden können.
- Entschlüsselung wird nur bei eingehenden E-Mails durchgeführt, wobei mit „eingehend" gemeint ist, dass der Domänenname der Absenderadresse nicht Bestandteil eines SMTP-Profils ist.Beispiel: Damit die Nachricht von der Adresse

`max.mustermann@beispiel.de` entschlüsselt wird, darf die Domäne `beispiel.de` *nicht* in den Routing-Einstellungen oder in irgendeinem SMTP-Profil angegeben sein.

- In die Betreffzeile jeder E-Mail wird eine Zusammenfassung des Signatur-/Verschlüsselungsergebnisses eingefügt. Beispiel: Einer E-Mail, die mit S/MIME korrekt signiert und verschlüsselt wurde, wird die Information „(S/MIME: Signed and encrypted) “ in der Betreffzeile angefügt.

Hinweis – Das Hinzufügen einer Fußzeile durch ein E-Mail-Programm (z. B. Microsoft Outlook oder Mozilla Thunderbird) zu Nachrichten, die bereits signiert oder verschlüsselt sind, zerstört die Signatur der E-Mails und macht sie damit ungültig. Wenn Sie digitale Zertifikate Client-seitig erzeugen wollen, deaktivieren Sie die Fußzeile der Antivirenprüfung. Wenn Sie jedoch nicht auf Datenschutz und Authentifizierung in Ihrer E-Mail-Kommunikation verzichten möchten und dennoch eine allgemeine Fußzeile für die Antivirenprüfung verwenden wollen, sollten Sie die integrierte Email-Encryption-Funktion von Sophos UTM einsetzen. Bei der Email Encryption auf dem Gateway wird die Fußzeile vor der digitalen Signierung zur Nachricht hinzugefügt, wodurch die Signatur intakt bleibt.

10.4.1 Allgemein

Auf der Registerkarte *Email Protection > Email Encryption > Allgemein* können Sie die Grundeinstellungen für die Email Encryption (E-Mail-Verschlüsselung) vornehmen.

Hinweis – Verschlüsselung funktioniert nur bei SMTP, nicht bei POP3.

Bevor Sie Email Encryption verwenden können, müssen Sie zunächst eine *Zertifizierungsstelle* (CA, Certificate Authority) erstellen. Diese CA besteht aus einem CA-Zertifikat und einem CA-Schlüssel. Das CA-Zertifikat kann heruntergeladen und lokal gespeichert werden.Es kann außerdem als externe CA (S/MIME-Instanz) in anderen Geräten installiert werden (siehe Diagramm), um eine transparente E-Mail-Verschlüsselung zwischen zwei Sophos UTM-Geräten zu ermöglichen.

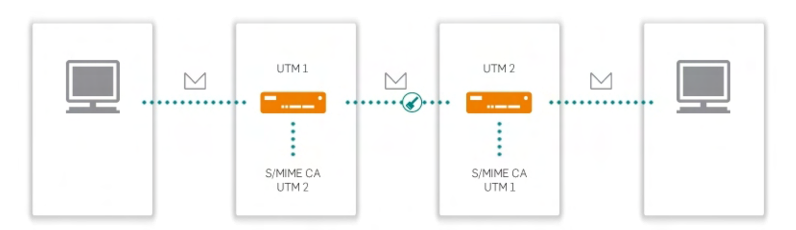


Bild 19 Email Encryption: Mit zwei Sophos UTM-Geräten

Um E-Mail-Verschlüsselung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die Email Encryption auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Zertifizierungsstelle (CA) für Email Encryption* kann nun bearbeitet werden.

2. **Erstellen Sie eine Zertifizierungsstelle (CA).**
   Füllen Sie das Formular *Zertifizierungsstelle (CA) für E-Mail-Verschlüsselung* aus. Standardmäßig ist das Formular mit den Werten von der Registerkarte *Verwaltung* > *Systemeinstellungen* > *Organisatorisches* vorausgefüllt.

3. **Klicken Sie auf *Speichern*.**
   Der Schieberegler wird grün und die folgenden Zertifikate bzw. Schlüssel werden generiert:

   - S/MIME-CA-Zertifikat
   - Öffnen Sie den PGP-Postmaster-Schlüssel.

   Beachten Sie, dass der Generierungsprozess einige Minuten dauern kann. Falls die Fingerabdrücke des S/MIME-CA-Zertifikats und des OpenPGP-Postmaster-Schlüssels nach einigen Minuten nicht anzeigt werden, klicken Sie auf die Schaltfläche *Aktualisieren* in der rechten oberen Ecke von WebAdmin. Das Zertifikat und der Schlüssel können heruntergeladen und lokal gespeichert werden.

Verwenden Sie die Schaltfläche *Email-Encryption-System jetzt zurücksetzen*, um alle Einstellungen im Menü *Email Encryption* in den Auslieferungszustand zurückzusetzen.

10.4.2 Optionen

Auf der Registerkarte *Email Encryption* > *Optionen* können Sie die Standardrichtlinie für die Public-Key-Verschlüsselung von Sophos UTM festlegen.

Standardrichtlinie: Legen Sie die Standardrichtlinie bezüglich der E-Mail-Verschlüsselung fest. Diese Einstellungen können allerdings durch benutzerspezifische Einstellungen überschrieben werden.

Die folgenden Aktionen sind möglich:

- Ausgehende E-Mails signieren
- Ausgehende E-Mails verschlüsseln
- Eingehende E-Mails verifizieren
- Eingehende E-Mails entschlüsseln

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Damit die Verschlüsselung funktioniert, muss der Absender in der Liste *Interne Benutzer* aufgeführt sein. Ausgehende E-Mails für Empfänger, deren S/MIME-Zertifikat oder öffentlicher OpenPGP-Schlüssel auf dem Gateway installiert ist, werden standardmäßig verschlüsselt. Wenn Sie Verschlüsselung für diese Empfänger deaktivieren wollen, löschen Sie deren S/MIME-Zertifikate oder öffentliche OpenPGP-Schlüssel. Wenn UTM Zertifikate oder öffentliche Schlüssel unbekannt sind, werden diese E-Mails unverschlüsselt versendet.

Automatische Extraktion von S/MIME-Zertifikaten

Wenn diese Option gewählt ist, werden die an eingehende E-Mails angehängten S/MIME-Zertifikate automatisch extrahiert. Voraussetzung hierfür ist, dass dieses Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurde, d. h. von einer CA, die auf dem Gerät vorhanden ist und deshalb unter *Email Protection* > *Email Encryption* > *S/MIME-CAs* angezeigt wird. Außerdem müssen Datum und Zeitpunkt von Sophos UTM innerhalb des Gültigkeitszeitraums des Zertifikats liegen, damit die automatische Extrahierung von Zertifikaten funktioniert. Erfolgreich extrahierte Zertifikate werden auf der Registerkarte *Email Protection* > *Email Encryption* > *S/MIME-Zertifikate* angezeigt. Beachten Sie, dass dieser Vorgang ca. fünf bis zehn Minuten dauern kann. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

OpenPGP-Schlüsselserver

OpenPGP-Schlüsselserver sind die Hosts für öffentliche PGP-Schlüssel. Sie können hier einen OpenPGP-Schlüsselserver angeben. Bei verschlüsselten eingehenden E-Mails oder bei ausgehenden E-Mails, die verschlüsselt werden sollen, versucht UTM, den öffentlichen Schlüssel vom angegebenen Server zu holen, wenn der entsprechende Schlüssel der UTM noch unbekannt ist.

10.4.3 Interne Benutzer

Um Nachrichten zu signieren und entschlüsseln, muss entweder der S/MIME-Schlüssel oder der private OpenPGP-Schlüssel auf der UTM vorhanden sein. Auf der Registerkarte *Email Encryption > Interne Benutzer* können Sie für die Benutzer, für die Email Encryption aktiviert werden soll, sowohl ein individuelles S/MIME-Schlüssel/Zertifikat-Paar als auch ein OpenPGP-Schlüsselpaar erstellen.

Um einen internen E-Mail-Benutzer hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Interne Benutzer* auf *Neuer E-Mail-Verschlüsselungsbenutzer*.**
   Das Dialogfeld *Neuen Benutzer erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   E-Mail-Adresse: Geben Sie die E-Mail-Adresse des Benutzers ein.

   Vor- und Nachname: Geben Sie den Namen des Benutzers ein.

   Signierung: Für die Signierung stehen die folgenden Optionen zur Auswahl:

   - Standardrichtlinie verwenden: Die auf der Registerkarte *Optionen* festgelegte Richtlinie wird verwendet.
   - Ein: E-Mails werden mit dem Zertifikat des Benutzers signiert.
   - Aus: E-Mails werden nicht signiert.

   Verschlüsselung: Für die Verschlüsselung stehen die folgenden Optionen zur Auswahl:

   - Standardrichtlinie verwenden: Die auf der Registerkarte *Optionen* festgelegte Richtlinie wird verwendet.
   - Ein: E-Mails werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
   - Aus: E-Mails werden nicht verschlüsselt.

   Verifizierung: Für die Verifizierung stehen die folgenden Optionen zur Auswahl:

   - Standardrichtlinie verwenden: Die auf der Registerkarte *Optionen* festgelegte Richtlinie wird verwendet.
   - Ein: E-Mails werden mit dem öffentlichen Schlüssel des Absenders verifiziert.
   - Aus: E-Mails werden nicht verifiziert.

Entschlüsselung: Für die Entschlüsselung stehen die folgenden Optionen zur Auswahl:

- Standardrichtlinie verwenden: Die auf der Registerkarte *Optionen* festgelegte Richtlinie wird verwendet.
- Ein: E-Mails werden mit dem Zertifikat des Benutzers entschlüsselt.
- Aus: E-Mails werden nicht entschlüsselt.

S/MIME: Sie können wählen, ob das S/MIME-Zertifikat und der Schlüssel automatisch vom System generiert werden sollen oder ob Sie ein Zertifikat im Format `PKCS#12` hochladen wollen. Wenn Sie das Zertifikat hochladen, müssen Sie das Kennwort kennen, mit dem die `PKCS#12`-Datei geschützt ist. Beachten Sie, dass die `PKCS#12`-Datei sowohl den S/MIME-Schlüssel als auch das Zertifikat enthalten muss. Jedes CA-Zertifikat, das eventuell zusätzlich in der `PKCS#12`-Datei enthalten ist, wird ignoriert.

OpenPGP: Sie können wählen, ob das OpenPGP-Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht, vom System automatisch generiert werden soll oder ob Sie das Schlüsselpaar im `ASCII`-Format hochladen wollen. Beachten Sie, dass der private und der öffentliche Schlüssel in einer einzigen Datei enthalten sein müssen und dass die Datei kein Kennwort enthalten darf.

> **Hinweis –** Falls Sie für einen Benutzer S/MIME und OpenPGP konfigurieren, werden die von ihm gesendeten E-Mails mittels S/MIME signiert.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Der neue Benutzer wird in der Liste *Interne Benutzer* angezeigt.

Verwenden Sie den Schieberegler, um die Benutzung eines oder beider Schlüssel abzuschalten, ohne die Schlüssel löschen zu müssen.

> **Hinweis –** Aus Sicherheitsgründen kann nur das S/MIME-Zertifikat bzw. der öffentliche Schlüssel aus dem OpenPGP-Schlüsselpaar heruntergeladen werden. Der S/MIME-Schlüssel und der private OpenPGP-Schlüssel können nicht vom System heruntergeladen werden.

10.4.4 S/MIME-CAs

Auf der Registerkarte *Email Encryption > S/MIME-CAs* können Sie die Zertifizierungsinstanzen (engl. certificate authorities, CAs) für die Email-Verschlüsselung verwalten. Zusätzlich zu den vorinstallierten CAs können Sie Zertifikate externer Zertifizierungsstellen hochladen. Allen eingehenden E-Mails, deren Zertifikate von einer der hier aufgelisteten aktiven CAs signiert sind, wird automatisch vertraut.

Hinweis – Wenn Sie die Option *Automatische Extraktion von S/MIME-Zertifikaten* auf der Registerkarte *Email Protection > Email Encryption > Optionen* ausgewählt haben, werden die Zertifikate der hier aufgelisteten aktiven CAs automatisch extrahiert und auf der Registerkarte *Email Protection > Email Encryption > S/MIME-Zertifikate* angezeigt.

Lokale S/MIME-CAs

Sie können Zertifikate (d. h. den öffentlichen Schlüssel) einer vertrauenswürdigen externen CA importieren. Auf diese Weise sind alle eingehenden E-Mails, deren Zertifikate von dieser CA signiert wurden, ebenfalls vertrauenswürdig. Sie können beispielsweise die CA eines anderen Sophos UTM-Geräts installieren. Dadurch ermöglichen Sie eine transparente E-Mail-Verschlüsselung zwischen beiden Sophos UTM.

Um eine externe S/MIME-CA zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf das Ordnersymbol neben dem Feld *Lokale CA hochladen*.**
   Das Dialogfeld *Datei hochladen* öffnet sich.

2. **Wählen Sie das Zertifikat aus, das Sie hochladen wollen.**
   Klicken Sie auf *Durchsuchen* und wählen Sie das CA-Zertifikat aus, das Sie hochladen wollen. Folgende Dateierweiterungen werden für Zertifikate unterstützt:

   - `cer`, `crt` oder `der`: Diese binären Zertifikattypen gleichen sich weitgehend.
   - `pem`: Base64-codierte DER-Zertifikate.

3. **Laden Sie das Zertifikat hoch.**
   Klicken Sie auf *Hochladen starten*, um das gewählte Zertifikat hochzuladen.

   Das Zertifikat wird installiert und im Bereich *Lokale S/MIME-CAs* angezeigt.

Sie können ein S/MIME-CA-Zertifikat löschen oder deaktivieren, wenn Sie es nicht mehr als vertrauenswürdig erachten. Um ein S/MIME-CA-Zertifikat zurückzuziehen, klicken Sie auf seinen Schieberegler. Der Schieberegler wird grau und der SMTP-Proxy akzeptiert ab jetzt keine E-

Mails mehr, die von dieser S/MIME-CA signiert sind. Um ein Zertifikat zu löschen, klicken Sie auf das Leeren-Symbol.

Tipp – Klicken Sie auf das blaue Infosymbol, um den Fingerabdruck der CA zu sehen.

Globale S/MIME-CAs

Die hier dargestellte Liste der S/MIME-CAs ist identisch mit den von Mozilla Firefox vorinstallierten S/MIME-CAs. Dies erleichtert die E-Mail-Verschlüsselung zwischen Ihrem Unternehmen und Ihren Kommunikationspartnern, die eine PKI (Public-Key-Infrastruktur) unterhalten, welche auf diesen CAs basiert. Sie können jedoch ein S/MIME-CA-Zertifikat deaktivieren, wenn Sie die CA nicht als vertrauenswürdig erachten. Um ein S/MIME-CA-Zertifikat zurückzuziehen, klicken Sie auf seinen Schieberegler. Der Schieberegler wird grau und der SMTP-Proxy akzeptiert ab jetzt keine E-Mails mehr, die von dieser S/MIME-CA signiert sind.

Nachfolgend sind einige URLs zu bekannten Zertifizierungsanbietern aufgeführt:

- Trustcenter
- S-TRUST
- Thawte
- VeriSign
- GeoTrust

10.4.5 S/MIME-Zertifikate

Auf der Registerkarte *Email Encryption > S/MIME-Zertifikate* können Sie externe S/MIME-Zertifikate importieren. E-Mails an Empfänger, deren Zertifikate auf dieser Registerkarte aufgeführt sind, werden automatisch verschlüsselt. Wenn für einen bestimmten Empfänger die E-Mails nicht verschlüsselt werden sollen, löschen Sie einfach das entsprechende Zertifikat aus der Liste.

Hinweis – Wenn für einen Empfänger neben dem S/MIME-Zertifikat auch ein OpenPGP-Schlüssel importiert wurde, werden die E-Mails mit OpenPGP verschlüsselt.

Hinweis – Wenn Sie ein S/MIME-Zertifikat manuell hochladen, wird Nachrichten von E-Mail-Adressen, die mit diesem Zertifikat verknüpft sind, immer vertraut – selbst wenn kein CA-

Zertifikat verfügbar ist, mit dem die Identität der Person auf dem Zertifikat überprüft werden könnte. Das bedeutet also, dass manuell hochgeladene S/MIME-Zertifikate immer als vertrauenswürdig gelten.

Um ein externes S/MIME-Zertifikat zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *S/MIME-Zertifikate* auf *Neues externes S/MIME-Zertifikat*.**
   Das Dialogfeld *S/MIME-Zertifikat hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Format: Wählen Sie das Format des Zertifikats. Sie können zwischen den folgenden Formaten wählen:

   - `der` (binär)
   - `pem` (ASCII)

   Hinweis – Microsoft-Windows-Betriebssysteme nutzen die Dateierweiterung `cer` für beide Formate (`der` und `pem`). Daher müssen Sie im Voraus wissen, ob es sich bei dem Zertifikat, das Sie hochladen wollen, um ein Binär- oder ASCII-Format handelt. Wählen Sie dann aus der Auswahlliste das entsprechende Format aus.

   Zertifikat: Klicken Sie auf das Ordnersymbol, um das Dialogfeld *Datei hochladen* zu öffnen. Wählen Sie die Datei aus und klicken Sie auf *Hochladen starten*.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Das neue S/MIME-Zertifikat wird in der Liste *S/MIME-Zertifikate* angezeigt.

10.4.6 OpenPGP-Schlüssel

Auf der Registerkarte *Email Encryption > OpenPGP-Schlüssel* können Sie öffentliche OpenPGP-Schlüssel installieren. Die Dateien müssen im `.asc`-Format vorliegen. Sie können auch ganze Schlüsselbunde (Keyrings) hochladen.

Hinweis – Importieren Sie keine Schlüsselbunddateien, die durch ein Kennwort geschützt sind.

Alle öffentlichen Schlüssel aus dem Schlüsselbund werden importiert und können dazu verwendet werden, Nachrichten zu verschlüsseln. E-Mails an Empfänger, deren öffentliche Schlüssel auf dieser Registerkarte aufgeführt sind, werden automatisch verschlüsselt. Wenn für einen bestimmten Empfänger die E-Mails nicht verschlüsselt werden sollen, löschen Sie einfach den entsprechenden öffentlichen Schlüssel aus der Liste.

Hinweis – Pro Schlüssel wird nur eine E-Mail-Adresse unterstützt. Falls einem Schlüssel mehrere E-Mail-Adressen zugeordnet sind, wird nur die „erste“ E-Mail-Adresse verwendet (die Reihenfolge kann von der Sortierung durch OpenPGP abhängen). Wenn Sie einen Schlüssel importieren möchten, der über mehrere E-Mail-Adressen verfügt, so müssen Sie vorher die unerwünschten Adressen mit OpenPGP oder einem anderen Programm entfernen, bevor Sie den Schlüssel in Sophos UTM importieren.

Um einen öffentlichen OpenPGP-Schlüssel zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *OpenPGP-Schlüssel* auf *Schlüsselbund importieren*.**
   Das Dialogfeld *OpenPGP-Schlüsselbund importieren* wird geöffnet.
2. **Laden Sie den/die OpenPGP-Schlüssel hoch.**
   Klicken Sie auf das Ordnersymbol, um das Dialogfenster *Datei hochladen* zu öffnen. Wählen Sie die Datei aus und klicken Sie auf *Hochladen starten*.

   Der Schlüssel oder (wenn die Datei mehrere Schlüssel enthält) die Liste von Schlüsseln wird angezeigt.
3. **Wählen Sie einen oder mehrere Schlüssel aus und klicken Sie auf *Gewählte Schlüssel importieren*.**
   Der/die Schlüssel werden in der Liste *OpenPGP-Schlüssel* angezeigt.

Hinweis – Dem Schlüssel muss eine E-Mail-Adresse zugeordnet sein. Ansonsten schlägt die Installation fehl.

10.5 SPX-Verschlüsselung

Bei der SPX-Verschlüsselung (Secure PDF Exchange) handelt es sich um die nächste Generation der E-Mail-Verschlüsselung. Sie ist clientlos und lässt sich sehr einfach einrichten und an eine beliebige Umgebung anpassen.Mithilfe von SPX-Verschlüsselung werden unverschlüsselte E-Mail-Nachrichten und Anhänge, die an die UTM gesendet werden, in ein PDF-Dokument umgewandelt, das dann mit einem Kennwort verschlüsselt wird.Sie können die UTM so konfigurieren, dass Absender Kennwörter für die Empfänger auswählen können oder der Server das Kennwort für den Empfänger generiert und für ihn aufbewahrt. Alternativ kann der Server einmalige Kennwörter für die Empfänger generieren.

Bei aktivierter SPX-Verschlüsselung können E-Mails auf zwei verschiedene Arten SPX-verschlüsselt werden:

- Der Administrator kann ein Plug-in für Microsoft Outlook herunterladen (siehe Kapitel *Email Protection* > *SPX-Verschlüsselung* > *SophosOutlook-Add-in*).Nach der Installation wird auf der Benutzeroberfläche von Microsoft Outlook die Schaltfläche *Verschlüsseln* angezeigt.Für die Verschlüsselung einer einzelnen Nachricht muss der Benutzer die Schaltfläche *Verschlüsseln* aktivieren und anschließend die Nachricht verfassen und abschicken. Eine Benachrichtigung wird nur gesendet (falls diese konfiguriert wurde), wenn beim Versand etwas schief geht, zum Beispiel wenn der Absender kein gültiges Kennwort eingibt.

  Hinweis – Wenn Sie Outlook nicht verwenden, können Sie die SPX-Verschlüsselung auch auslösen, indem Sie die Einstellung im Header-Feld X-Sophos-SPX-Verschlüsselung auf *ja* setzen.

- In der Funktion Data Protection können Sie festlegen, dass E-Mails mit vertraulichem Inhalt automatisch via SPX verschlüsselt werden (siehe Registerkarte *SMTP* > *Data Protection*).

Die verschlüsselte Nachricht wird daraufhin an den E-Mail-Server des Empfängers gesendet. Mithilfe von Adobe Reader kann der Empfänger die Nachricht entschlüsseln. Dazu ist das Kennwort erforderlich, das zum Verschlüsseln der PDF verwendet wurde. SPX-verschlüsselte E-Mail-Nachrichten können auf allen gängigen Smartphone-Plattformen, unter anderem Blackberry und Windows Mobile, mit nativer oder über Drittanbieter ermöglichter Unterstützung für PDF-Dateien abgerufen werden.

Mithilfe des SPX-Antwortportals kann der Empfänger sicher auf die E-Mail antworten.Es ist möglich, Ablaufzeiten für die sichere Antwort und nicht verwendete Kennwörter festzulegen (siehe Kapitel *Email Protection > SPX-Verschlüsselung > SPX-Konfiguration*).

Die SPX-Verschlüsselung kann in beiden SMTP-Konfigurationsmodi aktiviert werden, im einfachen Modus und im Profilmodus. Bei Nutzung des einfachen Modus kann eine globale SPX-Vorlage ausgewählt werden. Die SPX-Vorlage legt das Layout der PDF-Datei , die Kennworteinstellungen, die Empfängeranweisungen und die Einstellungen für das SPX-Antwortportal fest. Im Profilmodus können Sie verschiedene SPX-Vorlagen für unterschiedliche SMTP-Profile definieren. Wenn Sie also mehrere Kundendomänen verwalten, lassen sich benutzerdefinierte SPX-Vorlagen zuweisen, die beispielsweise unterschiedliche Unternehmenslogos und Texte enthalten können.

10.5.1 SPX-Konfiguration

Auf der Registerkarte *SPX Encryption > SPX-Konfiguration* können Sie die SPX-Verschlüsselung aktivieren und allgemeine Einstellungen für alle SMTP-Benutzer konfigurieren.

Um SPX-Verschlüsselung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die SPX-Verschlüsselung.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün.

2. **Legen Sie in den folgenden Abschnitten dieser Registerkarte die erforderlichen allgemeinen Einstellungen fest.**

3. **Bearbeiten Sie auf der Registerkarte *SPX-Vorlagen* die vorhandene Standardvorlage von Sophos und/oder fügen Sie neue SPX-Vorlagen hinzu.**

4. **Wählen Sie auf der Registerkarte *SMTP > Allgemein* die globale SPX-Vorlage aus.**

5. **Optional wählen Sie bei Verwendung des SMTP-Profilmodus die gewünschten SPX-Vorlagen für die entsprechenden SMTP-Profile aus.**

6. **Wenn Sie möchten, dass Benutzer E-Mail-Nachrichten mit Hilfe von SPX via Microsoft Outlook-Plugin verschlüsseln, achten Sie darauf, dass diese Benutzer Zugriff auf die Registerkarte *Email Protection > SPX-Verschlüsselung > Sophos Outlook-Add-in* haben. Wenn Sie einen anderen E-Mail-Messenger verwenden, müssen Sie den Header selbst manuell erstellen.**

SPX-Kennworteinstellungen

Mindestlänge: Die Mindestlänge der für ein Kennwort zulässigen Zeichen wird vom Absender festgelegt.

Erfordern Sonderzeichen: Bei Aktivierung dieser Option muss das vom Absender festgelegte Kennwort mindestens ein Sonderzeichen enthalten (nicht-alphanumerische Zeichen und Leerzeichen werden ebenfalls als Sonderzeichen behandelt).

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

SPX-Kennwortzurücksetzung

Kennwort zurücksetzen für: Hier können Sie das Kennwort eines Benutzers löschen.Geben Sie die E-Mail-Adresse des Empfängers ein und klicken Sie auf *übernehmen*.

SPX-Portaleinstellungen

Für SPX-Antwortportal verwendete Schnittstelle: Wählen Sie die Schnittstelle für das SPX-Antwortportal aus. Diese Webschnittstelle ermöglicht es den Empfängern SPX-verschlüsselter Nachrichten, dem Absender sicher zu antworten. In vielen Konfigurationen wäre dies die externe Schnittstelle.

Port: Geben Sie den Port an, den das SPX-Antwortportal überwachen soll.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Einstellungen für SPX-Portal und Kennwortablauf

Sichere Antwort zulassen für: Geben Sie an, wie lange der Empfänger einer SPX-verschlüsselten Nachricht eine Antwort über das SPX-Antwortportal versenden kann.

Nicht verwendetes Kennwort behalten für: Geben Sie die Ablaufzeit eines Kennworts ein, das zwischenzeitlich nicht verwendet wurde.

Hinweis – Wenn zum Beispiel nicht verwendetes Kennwort behalten auf 3 Tage eingestellt ist, läuft das Passwort um 0 Uhr aus, wenn für einen bestimmten Empfänger keine SPX-verschlüsselte Meldung verschickt wurde.

Hinweis – Wenn verwendetes Password behalten auf 0 Tage gesetzt ist, wird es gespeichert und um 0 Uhr ungültig.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

SPX-Benachrichtigungseinstellungen

Bei Fehler Benachrichtigung senden an: Legen Sie fest, wer beim Auftreten eines SPX-Fehlers benachrichtigt werden soll. Sie können die Benachrichtigung an den Administrator, den Absender oder an beide versenden oder keine Benachrichtigung verschicken. Fehlermeldungen werden immer im SMTP-Protokoll aufgelistet.

> **Tipp –** SPX-Fehlermeldungen können über die Registerkarte *Verwaltung > Anpassungen > E-Mail-Nachrichten* angepasst werden.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

10.5.2 SPX-Vorlagen

Auf der Registerkarte *SPX-Verschlüsselung > SPX-Vorlagen* können Sie die vorhandene Standardvorlage von Sophos bearbeiten und neue SPX-Vorlagen definieren.Bei Nutzung von SMTP im einfachen Modus kann für alle SMTP-Benutzer auf der Registerkarte *SMTP > Allgemein* eine globale SPX-Vorlage ausgewählt werden.Bei Nutzung von SMTP im Profilmodus können Sie verschiedene SPX-Vorlagen unterschiedlichen SMTP-Profilen auf der Registerkarte *SMTP Profile* zuweisen.

Um SPX-Verschlüsselung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Neue Vorlage*.**
   Das Dialogfenster *SPX-Vorlage erstellen* wird geöffnet.

   > **Tipp –** In der Standardvorlage von Sophos sind nützliche Einstellungen und Beispieltexte enthalten.Aus diesem Grund empfiehlt es sich, die vorhandene Vorlage mithilfe der Schaltfläche *Klonen* zu klonen, anstatt eine eigene Vorlage von Grund auf neu zu erstellen.

   > **Hinweis –** Beim Benachrichtigungsabsender handelt es sich um die E-Mail-Adresse, die unter *Verwaltung > Benachrichtigungen > Absender* konfiguriert wurde.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Vorlagenname: Geben Sie einen aussagekräftigen Namen für die Vorlage ein.

3. **Nehmen Sie die folgenden Grundeinstellungen vor:**
   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

   Unternehmensname: Der Unternehmensname wird in den Benachrichtigungen zu SPX aufgeführt, die je nach den vorgenommenen Einstellungen an den Administrator oder Absender der E-Mail versendet werden.

   PDF-Titelseite: Wählen Sie aus, ob der verschlüsselten PDF-Datei eine zusätzliche erste Seite hinzugefügt werden soll. Sie können die Standardseite oder eine benutzerdefinierte Seite verwenden. Wenn Sie eine benutzerdefinierte Seite verwenden möchten, laden Sie eine einseitige PDF-Datei mithilfe des Ordner-Symbols hoch.

   PDF-Verschlüsselung: Wählen Sie den Verschlüsselungsmodus der PDF-Datei aus. Beachten Sie, dass manche PDF-Viewer AES/256-verschlüsselte PDF-Dateien nicht lesen können.

   Bezeichnungssprachen: Wählen Sie die Anzeigesprache der Bezeichnungen für die an den Empfänger weitergeleitete E-Mail aus.Die E-Mail enthält Felder wie beispielsweise *Von*, *An*, *Absender* oder *Betreff*.

   Seitenformat: Wählen Sie das Seitenformat der PDF-Datei aus.

   Sophos-Logos entfernen: Aktivieren Sie diese Option, um das Sophos-Standardlogo durch das Logo Ihres Unternehmens zu ersetzen, das auf der Registerkarte *Verwaltung > Anpassungen > Allgemein* festgelegt wurde.Das Logo wird an zwei verschiedenen Stellen angezeigt: in der Fußzeile der an den Empfänger versandten verschlüsselten E-Mail und in der Fußzeile der Antwortnachricht, die über die Schaltfläche *Antworten* in der PDF-Datei generiert wird.

4. **Nehmen Sie die folgenden Kennworteinstellungen vor:**
   Kennworttyp: Wählen Sie aus, wie Sie das Kennwort für den Zugriff auf die verschlüsselte E-Mail-Nachricht generieren möchten. Unabhängig von der Auswahl muss der Absender immer dafür sorgen, dass das Kennwort sicher an den Empfänger übertragen wird.

   - **Von Absender festgelegt:** Wählen Sie diese Option, wenn der Absender der E-Mail das Kennwort selbst generieren soll.In diesem Fall muss der Absender das Kennwort in das Feld *Betreff* eingeben und dazu das folgende Format verwenden: `[secure:<Kennwort>]<Text der Betreffzeile>`, wobei `<Kennwort>` das Kennwort zum Öffnen der verschlüsselten PDF-Datei ist und

`<Text der Betreffzeile>` der gewünschte Betreff ist.Selbstverständlich wird das Kennwort von der UTM entfernt, bevor die E-Mail an den Empfänger gesendet wird.

> **Hinweis –** Eine Vorlage mit dieser Option sollte nicht in Verbindung mit Data Protection verwendet werden.Bei Data Protection weiß der Absender nicht im Voraus, dass eine E-Mail verschlüsselt wird, und gibt deshalb das Kennwort nicht in das Feld *Betreff* ein.Wenn die UTM versucht, eine E-Mail mithilfe von SPX zu verschlüsseln, ohne dass ein Kennwort angegeben wurde, erhält der Absender eine Fehlermeldung zum fehlenden Kennwort.

- **Generiert und für Empfänger gespeichert:** Die UTM erstellt automatisch ein empfängerspezifisches Kennwort, wenn die erste E-Mail an einen Empfänger gesendet wird. Dieses Kennwort wird an den Absender gesendet. Bei der nächsten E-Mail wird dasselbe Kennwort automatisch verwendet.Das Kennwort läuft ab, wenn es über einen bestimmten Zeitraum nicht verwendet wird, und kann vom Administrator zurückgesetzt werden, siehe Registerkarte *SPX-Konfiguration*.
- **Einmaliges Kennwort (OTP) für jede E-Mail generiert:** Die UTM erstellt für jede betroffene E-Mail automatisch ein neues Kennwort. Dieses Kennwort wird an den Absender gesendet.

Betreff der Benachrichtigung (nicht mit der Option *Von Absender festgelegt*): der Betreff der E-Mail, die von der UTM an den E-Mail-Absender versendet wird, mit dem Kennwort.Hier können Sie Variablen verwenden, z. B. `%%ENVELOPE_TO%%` für den Namen des Empfängers.

Benachrichtigungstext (nicht mit der Option *Von Absender festgelegt*): der Text der E-Mail, die von der UTM an den E-Mail-Absender versendet wird, mit dem Kennwort.Hier können Sie Variablen verwenden, z. B. `%%GENERATED_PASSWORD%%` für das Kennwort.

> **Tipp –** Die Standard-SPX-Vorlage von Sophos auf dieser Registerkarte enthält alle verfügbaren Variablen und ist ein hilfreiches Beispiel für eine Benachrichtigung.

5. **Nehmen Sie die folgenden Einstellungen für die Empfängeranweisungen vor:**
   Anweisungen für Empfänger: der Text der E-Mail, die von der UTM an den E-Mail-Empfänger versendet wird, mit Anweisungen in Bezug auf die verschlüsselte E-Mail.

Einfache HTML-Befehle und Hyperlinks sind gestattet.Sie können auch Variablen verwenden, z. B., `%%ORGANIZATION_NAME%%`.

> **Tipp –** Die Standard-SPX-Vorlage von Sophos auf dieser Registerkarte enthält alle verfügbaren Variablen und ist ein hilfreiches Beispiel für Empfängeranweisungen.

Bild für Kopfzeile/Bild für Fußzeile: Wählen Sie diese Option, wenn für die E-Mail von der UTM an den E-Mail-Empfänger ein Bild für die Kopf- und/oder Fußzeile verwendet werden soll. Sie können das Standardbild verwenden (ein orangefarbener Umschlag mit geeignetem Text) oder ein benutzerdefiniertes Bild auswählen. Wenn Sie ein benutzerdefiniertes Bild verwenden möchten, laden Sie eine JPG-, GIF- oder PNG-Datei mithilfe des Ordner-Symbols hoch. Die empfohlene Größe beträgt 752 x 69 Pixel.

6. **Nehmen Sie die folgenden SPX-Portaleinstellungen vor:**
   SPX-Antwortportal aktivieren: Bei Aktivierung enthält die an den Empfänger versendete, verschlüsselte PDF-Datei die Schaltfläche *Antworten*. Mithilfe dieser Schaltfläche kann der Empfänger das SPX-Antwortportal aufrufen und eine verschlüsselte E-Mail-Antwort an den Absender verschicken.

   Originaltext in Antwort übernehmen: Bei Aktivierung enthält die Antwort des Empfängers automatisch den Text der ursprünglichen E-Mail.

   Bild für Portal-Header/Bild für Portal-Fußzeile: Wählen Sie aus, ob für das SPX-Antwortportal ein Bild für die Kopf und/oder Fußzeile angezeigt werden soll. Sie können das Standardbild verwenden (ein orangefarbener Umschlag mit geeignetem Text) oder ein benutzerdefiniertes Bild auswählen. Wenn Sie ein benutzerdefiniertes Bild verwenden möchten, laden Sie eine JPG-, GIF- oder PNG-Datei mithilfe des Ordner-Symbols hoch. Die empfohlene Größe beträgt 752 x 69 Pixel.

7. **Klicken Sie auf *Speichern*.**
   Die SPX-Vorlage wird erstellt und in der Liste *SPX-Vorlagen* angezeigt.

Um eine SPX-Vorlage zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

10.5.3 SophosOutlook-Add-in

Auf der Registerkarte *Email Protection* > *SPX-Verschlüsselung* > *Sophos Outlook-Add-in* können Sie zur Website von Sophos navigieren und mithilfe Ihrer Anmeldeinformationen für

MySophos das Sophos Outlook-Add-in herunterladen.

Das Outlook-Add-in vereinfacht die Verschlüsselung von Nachrichten, die vertrauliche Inhalte enthalten und von Ihrem Unternehmen verschickt werden.Das Add-in und die Installationsdokumentation können Sie auf der Sophos Website herunterladen.

Führen Sie das Installationsprogramm mit folgenden Parametern aus: msiexec /qr /i SophosOutlookAddInSetup.msi T=1 EC=3 C=1 I=1

10.6 Quarantänebericht

Sophos UTMbesitzt eine E-Mail-Quarantäne, die alle Nachrichten enthält (SMTP und POP3), die aus verschiedenen Gründen blockiert und unter Quarantäne gestellt wurden. Das schließt Nachrichten ein, die auf ihre Zustellung warten, ebenso wie Nachrichten, die mit schädlicher Software infiziert sind, verdächtige Anhänge enthalten, als Spam identifiziert wurden oder einfach unerwünschte Ausdrücke enthalten.

Um das Risiko zu minimieren, dass Nachrichten irrtümlicherweise zurückgehalten werden (sogenannte *Fehlfunde*), sendet Sophos UTM an jeden Benutzer täglich einen Quarantänebericht, der über Nachrichten informiert, die sich in Quarantäne befinden. Benutzer mit mehreren E-Mail-Adressen erhalten einen individuellen Quarantänebericht für jede konfigurierte E-Mail-Adresse. Das gilt auch für zusätzliche POP3-Konten, die ein Benutzer im Benutzerportal konfiguriert hat, vorausgesetzt der POP3-Proxy von Sophos UTM befindet sich im *Vorabholenmodus*. Im Vorabholenmodus werden die E-Mails vom POP3-Server vorab abgerufen und in einer lokalen Datenbank abgelegt. Im Quarantänebericht kann der Benutzer auf eine Spam-E-Mail klicken, um diese Nachricht aus der Quarantäne freizugeben, oder er kann den Absender für zukünftige Nachrichten einer Whitelist (Positivliste) hinzufügen.

Die folgende Liste enthält weitere Informationen zum Quarantänebericht:

- Quarantäneberichte werden nur an Benutzer geschickt, deren E-Mail-Adresse zu einer Domäne gehört, die in einem SMTP-Profil enthalten ist. Dies beinhaltet sowohl die Angaben im Feld *Domänen* in auf der Registerkarte *SMTP* > *Routing* als auch die Angaben im Feld *Domänen* aller SMTP-Profile.
- Wenn die POP3-Option *Vorabholen* ausgeschaltet ist, werden Nachrichten in Quarantäne, die an dieses Konto geschickt wurden, nicht im Quarantänebericht aufgeführt. Stattdessen wird dem Benutzer die typische Sophos-Benachrichtigung über blockierte POP3-Nachrichten geschickt. Dadurch ist es dann nicht – wie über den

Quarantänebericht oder das Benutzerportal – möglich, die E-Mails freizugeben.Diese E-Mails können nur vom Administrator über den Mail-Manager im `zip`-Format heruntergeladen werden.

- Auf der Registerkarte *Erweitert* legt der Administrator fest, welche Typen von Quarantäne-E-Mails von den Benutzern freigegeben werden können. Standardmäßig können nur Spam-E-Mails aus der Quarantäne freigegeben werden.Nachrichten, die sich aus anderen Gründen in Quarantäne befinden, z. B. weil sie Viren oder verdächtige Dateianhänge enthalten, können nur vom Administrator über den Mail-Manager von Sophos UTM freigegeben werden. Außerdem können Benutzer all ihre Nachrichten in Quarantäne über das Benutzerportal von Sophos einsehen.
- Wenn eine Spam-E-Mail mehrere Empfänger hat, wie es oft bei Verteilerlisten (auch engl. mailing list) der Fall ist, und einer der Empfänger die E-Mail freigibt, wird die E-Mail nur für diesen Empfänger freigegeben, vorausgesetzt die E-Mail-Adresse der Verteilerliste ist auf dem System konfiguriert. Andernfalls wird die E-Mail an alle Empfänger gleichzeitig geschickt. Weitere Informationen finden Sie unter der Option *Interne Verteilerlisten definieren* auf der Registerkarte *Email Protection > Quarantänebericht > Ausnahmen*.
- E-Mails, die an eine SMTP-E-Mail-Adresse geschickt wurden, für die kein Benutzer auf Sophos UTM konfiguriert ist, können vom Administrator über den Quarantänebericht oder den Mail-Manager freigegeben (aber nicht auf die Whitelist gesetzt) werden. Da der Benutzer nicht konfiguriert ist, ist jedoch kein Zugriff über das Benutzerportal möglich.
- An Verteilerlisten geschickte Spam-Mails können grundsätzlich nicht einer Whitelist hinzugefügt werden.
- Einige E-Mail-Programme codieren den Header einer E-Mail nicht korrekt, was zu einer etwas merkwürdigen Darstellung dieser E-Mails im Quarantänebericht führen kann.

10.6.1 Allgemein

Auf der Registerkarte *Quarantänebericht > Allgemein* können Sie festlegen, zu welcher Zeit der tägliche Quarantänebericht versendet werden soll. Zusätzlich können Sie eine Nachricht schreiben, die an die Quarantäneberichte angehängt wird.

Um die Einstellungen für den Quarantänebericht zu bearbeiten, aktivieren Sie den Quarantänebericht.Klicken Sie auf den Schieberegler.
Der Schieberegler wird grün.

Zeitpunkt für den Berichtversand

Hier können Sie festlegen, wann der tägliche Quarantänebericht versendet werden soll.Wählen Sie die Zeit mit Hilfe der Auswahlliste aus und klicken Sie auf *Übernehmen*.
Sie können auch einen zusätzlichen Bericht versenden. Wählen Sie dazu die Option *Zusatzbericht senden*, stellen Sie die Zeit ein und klicken Sie auf *Übernehmen*.

Anpassbarer Nachrichtentext

Hier können Sie den Text anpassen, der als Einleitung des Quarantäneberichts dient. Ändern Sie den Nachrichtentext nach Ihren Wünschen und klicken Sie auf *Übernehmen*.

Hinweis – Es ist nicht möglich, HTML-Tags im Feld für den Nachrichtentext zu verwenden.

Hinweis – Anpassungen sind nicht möglich, wenn Sie eine Home-Use-Lizenz verwenden.

Hinweis – Beim Benachrichtigungsabsender handelt es sich um die E-Mail-Adresse, die unter *Verwaltung* > *Benachrichtigungen* > *Absender* konfiguriert wurde.

10.6.2 Ausnahmen

Auf der Registerkarte *Quarantänebericht* > *Ausnahmen* können Sie Ausnahmenlisten für E-Mail-Adressen definieren, um diese von den täglichen Quarantäneberichten auszunehmen.

Von Quarantäneberichten ausnehmen

Hier können Sie interne E-Mail-Adressen definieren, für die keine Quarantäneberichte versendet werden sollen. Benutzer, deren E-Mail-Adressen hier aufgeführt sind, erhalten keine täglichen Quarantäneberichte. Sie können vollständige E-Mail-Adressen eingeben oder einen Asterisk (*) als Platzhalter verwenden, z. B. `*@beispiel.de`.

Hinweis – Diese Ausnahmen gelten nur für den SMTP-Quarantänebericht. Wenn für einen Benutzer ein POP3-Konto angelegt ist, wird der POP3-Quarantänebericht trotzdem versendet.

Interne Verteilerlisten definieren

Wenn die E-Mail-Adresse einer Verteilerliste im Feld *Adress-Patterns von Verteilerlisten* konfiguriert ist (z. B. `newsletter@beispiel.de`) und eine Spam-E-Mail, die an diese Verteilerliste

gesendet wurde, entdeckt und unter Quarantäne gestellt wurde, dann wird der Quarantänebericht aller Empfänger dieser Verteilerliste einen Link zu dieser Spam-E-Mail enthalten. Dadurch kann jeder Empfänger die Spam-E-Mail für sich freigeben, indem er seine E-Mail-Adresse in das Dialogfenster eingibt, das angezeigt wird, wenn er auf den *Freigeben*-Link im Quarantänebericht geklickt hat.

Hinweis – Verteilerlisten können nicht über den Quarantänebericht oder das Benutzerportal auf die Whitelist (Positivliste) gesetzt werden.

Alternativ könnten Sie die E-Mail-Adresse dieser Verteilerliste einem lokalen Benutzer als zusätzliche E-Mail-Adresse in dessen Profil eintragen, wodurch dieser Benutzer zu einer Art Mail-Verwalter werden würde. Nur der Quarantänebericht dieses Benutzers besitzt dann einen Link zu der Spam-E-Mail, die an die Verteilerliste geschickt wurde. Ein Klick auf den *Freigeben*-Link würde dann die Spam-E-Mail an alle Empfänger der Verteilerliste auf einmal versenden.

Hinweis – Wenn die E-Mail-Adresse einer Verteilerliste als zusätzliche E-Mail-Adresse bei einem Benutzerprofil eingetragen ist, wird den übrigen Empfängern dieser Verteilerliste kein Freigeben-Link bei Spam-E-Mails angezeigt, die an diese Liste gesendet wurden.

Wenn die E-Mail-Adresse der Verteilerliste allerdings in einem Benutzerkonto als zusätzliche Adresse und gleichzeitig im Feld *Adress-Patterns von Verteilerlisten* eingetragen ist, dann wird im Quarantänebericht mit der Aktion *Freigeben* eine Eingabeaufforderung geöffnet. Der Benutzer kann dann bestimmen, wem die Spam-Mail zugestellt wird, indem er die entsprechende(n) E-Mail-Adresse(n) manuell in die Eingabeaufforderung einträgt.

Letztlich, wenn die E-Mail-Adresse der Verteilerliste weder als zusätzliche Adresse eines Benutzerkontos noch als Verteilerlisten-Adressmuster eingetragen ist, dann wird eine an diese Verteilerliste gesendete Spam-E-Mail wie eine normale E-Mail behandelt, d. h. wenn einer der Empfänger der Verteilerliste die Spam-E-Mail aus der Quarantäne freigibt, wird diese gleichzeitig auch an alle anderen Empfänger der Verteilerlisten geschickt.

Zusammenfassend gesagt, wann immer die E-Mail-Adresse einer Verteilerliste als Verteilerlisten-Adressmuster konfiguriert ist, erhält jeder Benutzer, der einen Freigabe-Link für die Spam-E-Mail in seinem Quarantänebericht hat, eine Eingabeaufforderung, in die er eine E-Mail-Adresse eingeben muss, an welche die Spam-E-Mail gesendet werden soll.

10.6.3 Erweitert

Auf der Registerkarte *Quarantänebericht > Erweitert* können Sie eine(n) alternative(n) Hostnamen und Portnummer für die *Freigeben*-Links im Quarantänebericht definieren. Zusätzlich können Sie die Freigabeoptionen für Spam-E-Mails ändern.

Erweiterte Optionen des Quarantäneberichts

Hostname: Standardmäßig ist der Hostname des Gateways voreingestellt, wie er auf der Registerkarte *Verwaltung > Systemeinstellungen > Hostname* angegeben ist. Der Quarantänebericht, der täglich vom Gateway verschickt wird, enthält Hyperlinks, auf die der Benutzer klicken kann, um eine Nachricht aus der Quarantäne freizugeben. Standardmäßig zeigen diese Links auf den hier angegebenen Hostnamen. Wenn Sie jedoch ermöglichen wollen, dass Benutzer ihre E-Mails über das Internet freigeben können, kann es notwendig sein, einen alternativen Hostnamen anzugeben, der öffentlich aufgelöst werden kann.

Port: Standardmäßig ist der Port `3840` eingestellt.Sie können den Port jedoch auf einen beliebigen Wert zwischen `1024` und `65535` ändern.

Zugelassene Netzwerke: Sie können auch Netzwerke angeben, denen gestattet ist, sich mit dem Freigabedienst zu verbinden. Standardmäßig ist nur das interne Netzwerk ausgewählt.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Freigabeoptionen

Hier können Sie auswählen, welche Arten von Nachrichten in Quarantäne durch Benutzer freigegeben werden dürfen. Sie können zwischen den folgenden Optionen wählen:

- Schadsoftware
- Spam
- Ausdruck
- Dateierweiterung
- Unscannbar
- MIME-Typ
- Andere

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

10.7 Mail-Manager

Der Mail-Manager ist ein administratives Werkzeug, mit dem alle E-Mails verwaltet und organisiert werden, die derzeit auf dem System gespeichert sind. Das schließt sowohl Nachrichten ein, die auf ihre Zustellung warten, als auch Nachrichten in Quarantäne, die mit schädlicher Software infiziert sind, verdächtige Anhänge enthalten, als Spam identifiziert wurden oder einfach unerwünschte Ausdrücke enthalten. Sie können den Mail-Manager dazu verwenden, alle Nachrichten einzusehen, bevor Sie sie herunterladen, freigeben oder löschen. Der Mail-Manager unterstützt UTF-8.

10.7.1 Mail-Manager-Fenster

Bild 20 Mail-Manager von Sophos UTM

Um das Fenster mit dem Mail-Manager zu öffnen, klicken Sie auf die Schaltfläche *Mail-Manager in neuem Fenster öffnen* auf der Registerkarte *Email Protection > Mail-Manager > Allgemein*. Der Mail-Manager ist in fünf Registerkarten unterteilt:

- **SMTP Quarantine:** Die SMTP-Quarantäne zeigt alle Nachrichten an, die momentan unter Quarantäne stehen.
- **SMTP Spool:** Zeigt alle Nachrichten an, die sich momentan in `/var/spool` befinden. Dies kann der Fall sein, wenn sie auf ihre Zustellung warten oder aufgrund eines Fehlers.
- **SMTP Log:** Das SMTP-Protokoll zeigt das Zustellungsprotokoll für alle Nachrichten, die über SMTP verarbeitet wurden.
- **POP3-Quarantäne:** Die POP3-Quarantäne zeigt alle Nachrichten an, die über POP3 geholt wurden und momentan unter Quarantäne stehen.
- **Close:** Klicken Sie hier, um das Mail-Manager-Fenster zu schließen.

10.7.1.1 SMTP-/POP3-Quarantäne

Nachrichten in der SMTP- und POP3-Quarantäne können so angezeigt werden, dass der Grund für ihren Quarantäneaufenthalt deutlich wird:

- Schadsoftware
- Spam
- Ausdruck
- Dateierweiterung
- MIME-Typ (nur SMTP)
- Unscannbar
- Andere

Verwenden Sie die Auswahlkästchen, um die Quarantäneursache auszuwählen. Doppelklicken Sie auf das Auswahlkästchen einer Ursache, um ausschließlich diese Ursache auszuwählen.

Tipp – Doppelklicken Sie auf eine Nachricht, um sie anzuschauen.

Profil/Domäne: Wählen Sie ein Profil oder eine Domäne aus, um nur dessen/deren Nachrichten zu sehen.

Abs./Empf./Betr.-Teilausdruck: Hier können Sie einen Absender, Empfänger oder Betreff eingeben (oder einen Wortteil davon), nach dem in den Nachrichten gesucht werden soll.

Eingangsdatum: Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Sie ein Datum ein oder wählen Sie ein Datum über das Kalendersymbol.

Sortieren nach: Standardmäßig wird die Liste nach Eingangsdatum sortiert. Nachrichten können nach Datum, Betreff, Absenderadresse und Nachrichtengröße sortiert werden.

und zeige: Sie können wählen, ob 20, 50, 100, 250, 500 oder 1000 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Verwenden Sie die Auswahlkästchen vor den Nachrichten oder klicken Sie auf Nachrichten um sie auszuwählen, und führen Sie dann Aktionen für die gewählten Nachrichten aus. Die folgenden Aktionen sind möglich:

- **Anzeigen** (nur für einzelne Meldungen verfügbar): Öffnet ein Fenster mit dem E-Mail-Inhalt.
- **Herunterladen:** Die gewählten Nachrichten werden heruntergeladen.
- **Löschen:** Die gewählten Nachrichten werden unwiderruflich gelöscht.
- **Freigeben:** Die gewählten Nachrichten werden aus der Quarantäne freigegeben.
- **Freigeben und als Fehlfund melden:** Die gewählten Nachrichten werden aus der Quarantäne freigegeben und als Fehlfund (false positive) an das Spam-Scan-Programm gemeldet.

Beachten Sie, dass nur der Administrator *alle* Nachrichten aus der Quarantäne freigeben kann.Benutzer, die ihre Nachrichten im Sophos Benutzerportal einsehen, können nur Nachrichten freigeben, für die ihnen das explizit gestattet ist. Die Autorisierungseinstellungen dafür finden Sie auf der Registerkarte *Email Protection* > *Quarantänebericht* > *Erweitert*.

Globale Aufräumaktion wählen: Hier finden Sie einige Löschoptionen, die auf alle Nachrichten global angewendet werden, das heißt, unabhängig davon, ob sie ausgewählt sind und/oder angezeigt werden oder nicht.

Warnung – Gelöschte Nachrichten können nicht wiederhergestellt werden.

10.7.1.2 SMTP-Spool

Hier sehen Sie Nachrichten, die entweder darauf warten, zugestellt zu werden, oder einen Fehler verursacht haben. Das Zustellungsprotokoll ist auch Teil des Headers einer Nachricht. Ver-

wenden Sie die folgenden Auswahlkästchen, um nur eine Sorte von Nachrichten zur Ansicht auszuwählen:

- **Ausstehend:** Nachrichten, deren Zustellung noch aussteht.
- **Fehler:** Nachrichten, die einen Fehler verursacht haben. Wenn eine Nachricht mehr als einmal einen Fehler verursacht, melden Sie den Fall bitte Ihrem Sophos Partner oder dem Sophos Support-Team.

Tipp – Doppelklicken Sie auf eine Nachricht, um sie anzuschauen.

Profil/Domäne: Wählen Sie ein Profil oder eine Domäne aus, um nur dessen/deren Nachrichten zu sehen.

Abs./Empf./Betr.-Teilausdruck: Hier können Sie einen Absender, Empfänger oder Betreff eingeben (oder einen Wortteil davon), nach dem in den Nachrichten gesucht werden soll.

Eingangsdatum: Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Sie ein Datum ein oder wählen Sie ein Datum über das Kalendersymbol.

Sortieren nach: Standardmäßig wird die Liste nach Eingangsdatum sortiert. Nachrichten können nach Datum, Betreff, Absenderadresse und Nachrichtengröße sortiert werden.

und zeige: Sie können wählen, ob 20, 50, 100, 250, 500 oder 1000 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Verwenden Sie die Auswahlkästchen vor den Nachrichten oder klicken Sie auf Nachrichten um sie auszuwählen, und führen Sie dann Aktionen für die gewählten Nachrichten aus. Die folgenden Aktionen sind möglich:

- **Herunterladen:** Die gewählten Nachrichten werden heruntergeladen.
- **Erneut versuchen:** Es wird sofort erneut versucht, die gewählten Nachrichten zuzustellen.
- **Löschen:** Die gewählten Nachrichten werden unwiderruflich gelöscht.
- **Zurückweisen:** Die gewählten Nachrichten werden zurückgewiesen, das heißt, der Absender erhält eine Nachricht, dass die Zustellung seiner Nachricht abgebrochen wurde, weil sie unzustellbar war.

Globale Aufräumaktion wählen: Hier finden Sie eine Wiederholungsoption sowie einige Löschoptionen, die auf alle Nachrichten global angewendet werden, das heißt, unabhängig davon, ob sie ausgewählt sind und/oder angezeigt werden oder nicht.

Warnung – Gelöschte Nachrichten können nicht wiederhergestellt werden.

10.7.1.3 SMTP-Protokoll

Das *SMTP-Protokoll* (SMTP Log) zeigt die Protokollmeldungen für alle über SMTP verarbeiteten Nachrichten.

Ergebnisfilter: Wählen Sie aus, welche Arten von Nachrichten angezeigt werden, indem Sie die entsprechenden Auswahlkästchen markieren.

- **Zugestellt:** Erfolgreich zugestellte Nachrichten.
- **Abgelehnt:** Nachrichten, die von der UTM abgelehnt wurden.
- **In Quarantäne:** Nachrichten, die unter Quarantäne gestellt wurden.
- **Verworfen:** Nachrichten, die ohne Benachrichtigung gelöscht wurden.
- **Abgebrochen:** Nachrichten, deren Zustellung manuell unter *SMTP Spool* abgebrochen wurde.
- **Zurückgewiesen:** Nachrichten, die nicht zugestellt werden konnten, aufgrund von z. B. falschen Routing-Einstellungen.
- **Gelöscht:** Manuell gelöschte Nachrichten.
- **Unbekannt:** Nachrichten, deren Status unbekannt ist.

Verwenden Sie die Auswahlkästchen, um *Ergebnisfilter*-Optionen an- oder abzuwählen. Doppelklicken Sie eine Option, um ausschließlich diese Option auszuwählen.

Ursachenfilter: Verwenden Sie die Auswahlkästchen, um das Nachrichtenprotokoll weiter zu filtern.

Hinweis – Doppelklicken Sie ein Nachrichtenprotokoll, um es anzuschauen. Klicken Sie auf das Serversymbol einer Nachricht, um die IP-Adresse aufzulösen. Ein Asterisk (*) kennzeichnet einen erfolgreichen Reverse-DNS-Lookup.

Profil/Domäne: Wählen Sie ein Profil oder eine Domäne aus, um nur dessen/deren Nachrichten zu sehen.

IP/Netz/Adresse/Betr. -Teilausdruck: Hier können Sie eine IP-Adresse, Netzwerkadresse oder einen Betreff eingeben, um danach in den SMTP-Protokollmeldungen zu suchen.

Eingangsdatum: Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Sie ein Datum ein oder wählen Sie ein Datum über das Kalendersymbol.

Sortieren nach: Standardmäßig wird die Liste nach Ereignisdatum sortiert. Nachrichten können nach Ereignisdatum, Absenderadresse und Nachrichtengröße sortiert werden.

und zeige: Sie können wählen, ob 20, 50, 100, 250, 500 oder 1000 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite.Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

10.7.2 Allgemein

Im oberen Bereich der Registerkarte *Mail-Manager > Allgemein* können Sie den Mail-Manager öffnen, indem Sie auf die Schaltfläche *Mail-Manager in neuem Fenster öffnen* klicken.

Im unteren Bereich bietet der Abschnitt *Statistischer Überblick* eine Übersicht über alle Nachrichten, die augenblicklich auf dem System gespeichert sind. Die Daten sind unterteilt in Nachrichten, die über SMTP, und solche, die über POP3 zugestellt wurden. Für beide Arten werden die folgenden Informationen angezeigt:

- **Warten auf Auslieferung (spooled)** (nur SMTP): Hierbei handelt es sich um Mails, die sich in Spool befinden, z. B. weil sie gescannt wurden und bis jetzt noch nicht ausgeliefert werden konnten.
- **Legitime Nachrichten insgesamt** (nur POP3): Mails, die vom System vorab geholt wurden und bisher noch nicht von einem Client/Benutzer abgeholt wurden.
- **Schadsoftware in Quarantäne:** Die Anzahl an Nachrichten, die Schadsoftware enthalten, wie z. B. Viren oder anderen schädlichen Inhalt.
- **Spam in Quarantäne:** Die Anzahl an Nachrichten, die als Spam identifiziert und deshalb unter Quarantäne gestellt wurden.
- **Ausdruck in Quarantäne:** Die Anzahl an Nachrichten, die unter Quarantäne gestellt wurden, weil sie unerwünschte Ausdrücke enthalten.
- **Dateierweiterung in Quarantäne:** Die Anzahl an Nachrichten, die unter Quarantäne stehen, weil sie verdächtige Dateianhänge (die über ihre Dateierweiterung identifiziert wurden) enthalten.

- **Unscannbarer Inhalt in Quarantäne:** Die Anzahl an Nachrichten, die unter Quarantäne stehen, weil sie nicht gescannt werden konnten.
- **MIME-Typ in Quarantäne** (nur SMTP): Die Anzahl an Nachrichten, die unter Quarantäne stehen, weil sie einen MIME-Typ haben, der laut den SMTP-Einstellungen gefiltert werden soll.
- **In Quarantäne insgesamt:** Die Gesamtzahl an Nachrichten, die unter Quarantäne stehen.

Hinweis – Die Zahlen für *Warten auf Auslieferung* geben einen Echtzeit-Ausschnitt der SMTP-Nachrichten wieder. Für POP3-Nachrichten hingegen beschreiben die Zahlen die Daten, die seit dem letzten Vorabholen aufgelaufen sind.

Unten sehen Sie eine kurze Statistik über die SMTP-Quarantäne und die Ablehnungen der letzten 24 Stunden:

- **Schadsoftware in Quarantäne/abgelehnt:** Nachrichten, die unter Quarantäne gestellt oder abgelehnt wurden, weil sie schädlichen Inhalt besitzen.
- **Spam in Quarantäne/abgelehnt:** Nachrichten, die unter Quarantäne gestellt oder abgelehnt wurden, weil sie als Spam identifiziert wurden.
- **Ablehnungen durch Blacklist:** Nachrichten, die abgelehnt wurden, weil ihr Absender auf der Blacklist geführt wird.
- **Ablehnungen nach Adressüberprüfung:** Nachrichten, die abgelehnt wurden, weil ihre Absenderadresse nicht verifiziert werden konnte.
- **Ablehnungen durch SPF:** Nachrichten, die abgelehnt wurden, weil der sie sendende Host nicht zugelassen ist.
- **Ablehnung durch RBL:** Nachrichten, die abgelehnt wurden, weil der Absender auf einer Echtzeit-Blackhole-Liste geführt wird.
- **Ablehnungen durch BATV:** Nachrichten, die abgelehnt wurden, weil das BATV-Tag ungültig war.
- **Ablehnungen durch RDNS/HELO:** Nachrichten, die abgelehnt wurden, weil das HELO ungültig war oder RDNS-Einträge fehlten.

Ob es überhaupt Ablehnungen gibt, hängt von Ihren Einstellungen unter *Email Protection > SMTP* ab.

10.7.3 Konfiguration

Auf der Registerkarte *Mail-Manager > Konfiguration* wird definiert, nach wie vielen Tagen das Datenbankprotokoll geleert beziehungsweise die unter Quarantäne gestellten E-Mails gelöscht werden. Alle Protokolle und E-Mails, die älter sind als die hier eingestellte Anzahl an Tagen, werden automatisch gelöscht.

Die Voreinstellungen sehen folgendermaßen aus:

- Das Datenbankprotokoll wird nach drei Tagen geleert. Die maximal erlaubte Anzahl an Tagen beträgt 30 Tage.
- Nachrichten in Quarantäne werden nach 14 Tagen gelöscht. Die maximal erlaubte Anzahl an Tagen beträgt 999 Tage.

Die minimal erlaubte Anzahl an Tagen für sowohl das Datenbankprotokoll als auch die Quarantäne beträgt einen Tag.

Datenbankprotokoll leeren

Diese Option ist nützlich, wenn sich im Datenbankprotokoll eine enorme Menge an Daten angesammelt hat und Sie das Protokoll sofort leeren möchten. Auf diese Weise müssen Sie nicht warten, bis die normale Aufräumaktion durchgeführt wird.

11 Endpoint Protection

Über das Menü *Endpoint Protection* können Sie den Schutz der Endpoints in Ihrem Netzwerk verwalten, z. B. von Desktop-Computern, Servern und Laptops. UTM ist die Stelle, an der Sie Endpoint Protection konfigurieren; hier laden Sie die Software für Endpoints herunter, verschaffen sich einen Überblick über die geschützten Endpoints, richten Antiviren- und Device-Control-Richtlinien ein, gruppieren Endpoints und ordnen die definierten Richtlinien den Endpoint-Gruppen zu.

Endpoint Protection nutzt den zentralen Dienst Sophos LiveConnect. Dieser Cloud-basierte Dienst wird automatisch für die Verwendung mit UTM konfiguriert, wenn Sie Endpoint Protection aktivieren. LiveConnect ermöglicht Ihnen jederzeit die Verwaltung von Endpoints in Ihrem lokalen Netzwerk, an entfernten Standorten oder bei mobilen Benutzern. Der LiveConnect-Dienst umfasst Folgendes:

- Ein vorkonfiguriertes Installationspaket für den Endpoint-Agent
- Richtlinienumsetzung und Aktualisierungen für Endpoints
- Sicherheitsaktualisierungen und Definitionen für Endpoints
- Zentrale Protokoll- und Berichtsdaten zur zentralen Überwachung von Endpoints über WebAdmin

Da es sich bei LiveConnect um einen Cloud-basierten Dienst handelt, benötigen Sie eine aktive Internetverbindung, um den Dienst nutzen zu können. Verwaltete Endpoints benötigen ebenfalls eine Internetverbindung, um Richtlinien- und Sicherheitsaktualisierungen empfangen zu können.

Die Abbildung unten zeigt ein Beispiel für die Implementierung von Sophos UTM Endpoint Protection mit Nutzung des LiveConnect-Diensts.

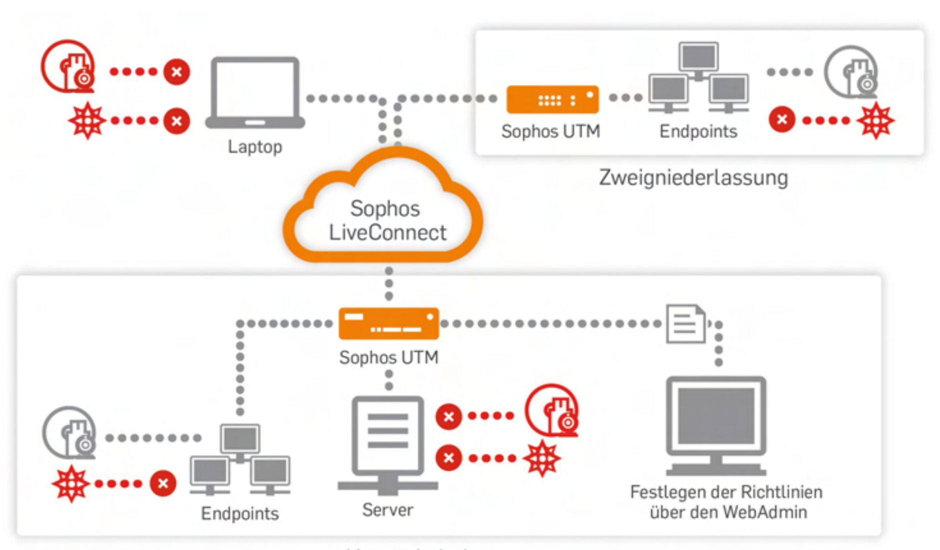


Bild 21 Endpoint Protection: Übersicht

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Computerverwaltung
- Antivirus
- Device Control

Wenn Endpoint Protection aktiviert ist, werden auf der Übersichtsseite allgemeine Informationen zu registrierten Computern und deren Status angezeigt. Sie können diese Liste sortieren und durchsuchen. Wenn der Status eines Endpoints nicht *OK* lautet, können Sie den Status anklicken, um ein Fenster mit weiteren Informationen zu öffnen. Der Status *Keine Übereinstimmung* weist darauf hin, dass die Geräteeinstellungen derzeit nicht mit der Konfiguration von UTM übereinstimmen. Um dieses Problem zu beheben, müssen Sie über einen Link im Fenster die aktuellen Endpoint-Einstellungen an den Endpoint senden. Für andere Status können Sie die Informationen bestätigen und entscheiden, welche Maßnahmen erforderlich sind.

Endpoint Protection Live-Protokoll öffnen

Das Live-Protokoll von Endpoint Protection stellt Informationen über die Verbindungen zwischen den Endpoints, LiveConnect und UTM sowie Sicherheitsinformationen über die

Endpoints bereit. Klicken Sie auf die Schaltfläche *Endpoint-Protection-Live-Protokoll öffnen*, um das Live-Protokoll in einem neuen Fenster zu öffnen.

11.1 Computerverwaltung

Auf den Seiten *Endpoint Protection* > *Computerverwaltung* können Sie den Schutz für einzelne Computer, die mit Ihrer Sophos UTM verbunden sind, aktivieren und verwalten.

Sie können nach einer Installationsdatei für Endpoints suchen und diese verwenden und sich einen Überblick über alle Computer verschaffen, auf denen Endpoint Protection installiert ist. Sie können Computergruppen mit abweichenden Schutzeinstellungen definieren.

11.1.1 Allgemein

Auf der Registerkarte *Endpoint Protection* > *Computerverwaltung* > *Allgemein* können Sie Endpoint Protection aktivieren und deaktivieren.

Um Endpoint Protection zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Endpoint Protection auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und einige Felder mit Details zu Ihrer Organisation werden angezeigt.

2. **Geben Sie Informationen zu Ihrer Organisation ein.**
   Standardmäßig werden die Einstellungen von der Registerkarte *Verwaltung* > *Systemeinstellungen* > *Organisatorisches* verwendet.

3. **Optional können Sie einen übergeordneten Proxy konfigurieren:**
   Wenn Ihr UTM keinen direkten HTTP-Internetzugang hat, kann Endpoint Protection einen Proxy-Server verwenden, um Sophos LiveConnect zu erreichen. Wählen Sie *Übergeordneten Proxy verwenden* und geben Sie gegebenenfalls den Host und den Port ein.

4. **Klicken Sie auf *Endpoint Protection aktivieren*.**
   Der Schieberegler wird grün und Endpoint Protection wird aktiviert.

   Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

Auf der Seite *Agent installieren* können Sie nun im nächsten Schritt den zu überwachenden Computern ein Endpoint-Protection-Installationspaket bereitstellen.

Hinweis – Wenn Sie Endpoint Protection verwenden, empfehlen wir Ihnen, die Option *Zwischenspeichern für Sophos-Endpoint-Aktualisierung erzwingen* auf der Registerkarte *Web Protection* > *Filteroptionen* > *Sonstiges*, Bereich *Webfilter-Zwischenspeicherung*, zu aktivieren, um Uplink-Engpässe zu vermeiden, wenn Endpoints Daten von den Update-Servern im Internet herunterladen.

Hinweis – Der Administrator kann Alarmmeldungen für die Endpoint-Viruserkennung auf der Registerkarte *Verwaltung* > *Benachrichtigungen* > *Benachrichtigungen*, Bereich *Endpoint* konfigurieren.

Hinweis – Wenn der Webfilter und der transparente Modus aktiv sind, sind zusätzliche Einstellungen erforderlich, um sicherzustellen, dass Endpoint Protection wie vorgesehen an den Endpoints eingesetzt werden kann: Wenn Endpoint Protection aktiviert ist, erstellt die UTM die DNS-Gruppe *Sophos LiveConnect* automatisch. Fügen Sie diese DNS-Gruppe im Feld *Transparenzmodus-Zielhosts/-netze ausnehmen* auf der Registerkarte *Web Protection* > *Filteroptionen* > *Sonstiges* hinzu.

Um Endpoint Protection zu deaktivieren, gehen Sie folgendermaßen vor:

1. **Deaktivieren Sie Endpoint Protection auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und zwei Optionen werden angezeigt.

2. **Entscheiden Sie, ob Sie Ihre Endpoint-Daten löschen möchten.**
   ALLE Daten beibehalten: Wählen Sie diese Option, wenn Sie Endpoint Protection vorübergehend deaktivieren möchten. Ihre Endpoint-Einstellungen werden gespeichert. Wenn Sie die Funktion erneut aktivieren, wird automatisch eine Verbindung mit den bereits installierten Endpoints hergestellt und alle festgelegten Richtlinien stehen zur Verfügung.

   ALLE Daten löschen: Wählen Sie diese Option, wenn Sie alle Endpoint-Einstellungen zurücksetzen und von vorne beginnen möchten. Alle Verbindungen mit Endpoints und alle Richtlinieneinstellungen werden gelöscht. Nachdem Sie die Funktion erneut aktiviert haben, installieren Sie neue Installationspakete an den Endpoints, damit die neuen Registrierungsdaten dort verfügbar sind (siehe Abschnitt *Computerverwaltung* > Erweitert).

3. **Klicken Sie auf *Endpoint Protection deaktivieren*.**

Der Schieberegler wird grau und Endpoint Protection wird deaktiviert.

11.1.2 Agent installieren

Auf der Registerkarte *Endpoint Protection* > *Computerverwaltung* > *Agent installieren* können Sie die Installationsdateien für die Computer, die von Endpoint Protection überwacht werden sollen, herunterladen.

Die beiden Pakete bieten zwei verschiedene Möglichkeiten, Endpoint Protection an Endpoints zu installieren:

- Klicken Sie zum Herunterladen und Speichern des Installationspakets auf die Schaltfläche *Kompakt-Installation herunterladen*. Geben Sie dann den Endpoint-Benutzern Zugriff auf das Paket.
- Kopieren Sie die URL aus dem grauen Feld und senden Sie sie an die Endpoint-Benutzer. Über diese URL können die Endpoint-Benutzer das Installationspaket selbst herunterladen und installieren.

Hinweis – Der Name der Installationspakete darf nicht geändert werden. Während der Installation vergleicht LiveConnect den Paketnamen mit den aktuellen Registrierungsdaten der UTM. Wenn die Informationen nicht übereinstimmen, wird der Installationsvorgang abgebrochen.

Nach der Installation am Endpoint wird der jeweilige Computer auf der Registerkarte *Computer verwalten* angezeigt. Außerdem wird er der Computergruppe, die auf der Registerkarte *Erweitert* festgelegt wurde, automatisch zugewiesen.

Hinweis – Das Installationspaket kann mit Hilfe der Schaltfläche *Registrierungstoken zurücksetzen* auf der Registerkarte *Erweitert* ungültig gemacht werden.

11.1.3 Computer verwalten

Auf der Registerkarte *Endpoint Protection* > *Computerverwaltung* > *Computer verwalten* erhalten Sie einen Überblick über die Computer, auf denen Endpoint Protection für Ihre UTM installiert ist. Die Computer werden automatisch zur Liste hinzugefügt. Sie können einen Computer einer Gruppe zuweisen, weitere Informationen hinzufügen, den Manipulationsschutz eines Computers ändern oder einen Computer aus der Liste löschen.

Um die Einstellungen eines Computer auf der Liste zu ändern, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Bearbeiten* des betreffenden Computers.**
   Das Dialogfeld *Computer bearbeiten* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Computergruppe: Wählen Sie die Computergruppe aus, der Sie den Computer zuweisen möchten. Der Computer erhält die Schutzeinstellungen der Gruppe, der er zugewiesen ist.

   Typ: Wählen Sie einen Computertyp, also Desktop, Laptop oder Server. Die Zuweisung eines Typs ist bei der Filterung der Liste hilfreich.

   Manipulationsschutz: Wenn der Manipulationsschutz aktiviert ist, können die Schutzeinstellungen eines Computers lokal nur durch Eingabe eines Kennworts geändert werden. Das Kennwort wird auf der Registerkarte *Erweitert* festgelegt. Wenn diese Funktion deaktiviert ist, kann der Endpoint-Benutzer die Schutzeinstellungen ohne Eingabe eines Kennworts ändern. Standardmäßig stimmen die Einstellungen mit den Einstellungen der Gruppe überein, der der Computer zugeordnet ist.

   Bestandsnr. (optional): Geben Sie die Bestandsnummer des Computers ein.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.

Um einen Computer aus der Liste zu löschen, klicken Sie auf die Schaltfläche *Löschen*.

Hinweis – Wenn Sie einen Computer aus der Liste löschen, wird er nicht mehr von der UTM überwacht. Die installierte Endpoint-Software wird jedoch nicht automatisch deinstalliert und die zuletzt angewandten Richtlinien bleiben aktiv.

11.1.4 Gruppen verwalten

Auf der Registerkarte *Endpoint Protection* > *Computerverwaltung* > *Gruppen verwalten* können Sie die geschützten Computer zu Gruppen zusammenfassen und gruppenweite Endpoint Protection-Einstellungen festlegen. Alle Computer, die einer Gruppe angehören, verfügen über die gleichen Antiviren- und Geräte-Richtlinien.

Hinweis – Jeder Computer ist genau einer Gruppe zugeordnet. Anfangs sind alle Computer der Standardgruppe zugeordnet. Nachdem Sie Gruppen hinzugefügt haben, können Sie auf der Registerkarte *Erweitert* festlegen, welche Gruppe Sie als Standardgruppe verwenden möchten, d. h. welcher Gruppe neu installierte Computer automatisch zugeordnet werden.

Um eine Computergruppe anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Computergruppe hinzufügen*.**
   Das Dialogfeld *Computergruppe hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Gruppe ein.

   Antivirus-Richtlinie: Wählen Sie die Antivirus-Richtlinie, die für diese Gruppe gelten soll. Die Richtlinien sind auf der Registerkarte *Antivirus* > *Richtlinien* definiert. Beachten Sie, dass Sie auf der Registerkarte *Antivirus* > *Ausnahmen* gruppenspezifische Ausnahmen von dieser Richtlinie festlegen können.

   Geräterichtlinie: Wählen Sie die Geräterichtlinie, die für diese Gruppe gelten soll. Die Richtlinien sind auf der Registerkarte *Device Control* > *Richtlinien* definiert. Beachten Sie, dass Sie auf der Registerkarte *Device Control* > *Ausnahmen* gruppenspezifische Ausnahmen von dieser Richtlinie festlegen können.

   Manipulationsschutz: Wenn der Manipulationsschutz aktiviert ist, können die Schutzeinstellungen der jeweiligen Endpoints lokal nur durch Eingabe eines Kennworts geändert werden. Das Kennwort wird auf der Registerkarte *Erweitert* festgelegt. Wenn diese Funktion deaktiviert ist, kann der Endpoint-Benutzer die Schutzeinstellungen ohne Eingabe eines Kennworts ändern. Beachten Sie, dass Sie die Schutzeinstellungen für einzelne Computer auf der Registerkarte *Computer verwalten* ändern können.

   Web Control: Wenn diese Option aktiv ist, können Endpoints dieser Gruppe Webfilterrichtlinien erzwingen und über diese berichten, selbst wenn sie sich nicht in einem Sophos UTM-Netzwerk befinden. Endpoint-Web-Control aktivieren Sie auf der Registerkarte *Endpoint Protection* > *Web Control*.

   Proxy für AutoUpdate verwenden: Ist diese Option aktiviert, werden die darunter festgelegten Proxy-Attribute an die Endpoints dieser Gruppe gesendet. Die Endpoints verbinden sich mit Hilfe dieser Proxy-Daten mit dem Internet.

Hinweis – Stellen Sie sicher, dass Sie die korrekten Daten eingeben. Wenn die Endpoints falsche Proxy-Daten erhalten, können sie sich nicht mehr mit dem Internet und mit der UTM verbinden. In diesem Fall müssen Sie die Konfiguration auf jedem betroffenen Endpoint manuell anpassen.

Adresse: Geben Sie die IP-Adresse des Proxys ein.

Port: Geben Sie die Port-Nummer des Proxys ein.

Benutzer: Geben Sie bei Bedarf den Benutzernamen des Proxys ein.

Kennwort: Geben Sie bei Bedarf das Kennwort des Proxys ein.

Computer: Fügen Sie die Computer hinzu, die zur Gruppe gehören sollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die Gruppe wird erstellt und in der Liste *Gruppen verwalten* angezeigt. Bitte beachten Sie, dass es bis zu 15 Minuten dauern kann, bis alle Computer neu konfiguriert sind.

Um eine Gruppe zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

11.1.5 Erweitert

Auf der Registerkarte *Endpoint Protection* > *Computerverwaltung* > *Erweitert* können die folgenden Optionen konfiguriert werden:

Manipulationsschutz: Wenn der Manipulationsschutz aktiviert ist, können Schutzeinstellungen nur an Endpoints, die dieses Kennwort verwenden, geändert werden.

Standard-Computergruppe: Wählen Sie direkt nach der Installation von Endpoint Protection die Computergruppe aus, der ein Computer automatisch zugewiesen wird.

Sophos LiveConnect – Registrierung: Dieser Abschnitt enthält Informationen zur Registrierung von Endpoint Protection. Die Informationen werden unter anderem zur Identifikation von Installationspaketen und für Supportzwecke verwendet.

Wenn Sie Sophos Enterprise Console zur Verwaltung von Endpoints verwenden, können Sie dieses UTM zur Bereitstellung ihrer Web Control-Richtlinie verwenden. *Kopieren Sie unter*

SEC-Informationen den *Hostnamen* und den *Geteilten Schlüssel* in den Web Control-Richtlinieneditor in Sophos Enterprise Console.

- **Registrierungstoken zurücksetzen**: Klicken Sie auf diese Schaltfläche, um zu verhindern, dass Endpoints mit einem bereits verwendeten Installationspaket installiert werden. Dies erfolgt typischerweise zum Abschluss eines Rollouts. Wenn Sie möchten, dass neue Endpoints installiert werden können, stellen Sie ein neues Installationspaket über die Registerkarte *Agent installieren* zur Verfügung.

Übergeordneter Proxy: Verwenden Sie einen übergeordneten Proxy, wenn Ihre UTM keinen direkten Internetzugriff bietet.

11.2 Antivirus

Auf den Seiten *Endpoint Protection > Antivirus* legen Sie die Antiviren-Einstellungen für Endpoint Protection fest. Sie können Antiviren-Richtlinien, also bestimmte Zusammenstellungen von Antiviren-Einstellungen, erstellen und diese auf Ihre Computergruppen anwenden, die von Endpoint Protection überwacht werden. Sie können auch Ausnahmen von den Antiviren-Funktionen definieren, die nur für bestimmte Computergruppen gelten.

11.2.1 Richtlinien

Auf der Registerkarte *Endpoint Protection > Antivirus > Richtlinien* können Sie verschiedene Antivirus-Einstellungen verwalten und auf die von Endpoint Protection überwachten Computergruppen anwenden.

Die Antiviren-Standardrichtlinie *Basic protection* bietet die beste Balance aus Sicherheit für Ihren Computer und allgemeiner Systemleistung. Sie kann nicht angepasst werden.

Um eine neue Antiviren-Richtlinie hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Richtlinie hinzufügen*.**
   Das Dialogfeld *Richtlinie hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Richtlinie ein.

   Zugriffsscan: Aktivieren Sie diese Option, wenn Dateien bei jedem Kopieren, Verschieben oder Öffnen gescannt werden sollen. Der Zugriff auf Dateien wird nur gewährt, wenn sie keine Gefahr darstellen oder sie zur Verwendung autorisiert wurden.

- **PUA-Scan:** Aktivieren Sie diese Option, um beim Zugriffsscan auch nach potenziell unerwünschten Anwendungen (PUAs) zu suchen.

Automatische Bereinigung: Aktivieren Sie diese Option, um infizierte Dateien oder Spyware automatisch zu bereinigen. Dateien mit Schadsoftware werden gelöscht, infizierte Dateien werden gesäubert. Die so bereinigten Dateien sind irreparabel beschädigt, da der Virenscanner den ursprünglichen Zustand der Datei vor ihrer Infektion nicht wiederherstellen kann.

Sophos Live Protection: Wenn der Antiviren-Scan auf einem Endpoint-Computer eine verdächtige Datei erkennt, anhand der auf dem Computer gespeicherten Sophos-Definitionsdateien (IDE) aber nicht entscheiden kann, ob die Datei sauber oder infiziert ist, werden bestimmte Dateiinformationen (wie die Prüfsumme und andere Attribute) an Sophos gesendet, um die weitere Analyse zu ermöglichen.

Bei dieser Cloud-basierten Überprüfung wird die SophosLabs-Datenbank nach Informationen über die verdächtige Datei durchsucht. Wenn die Datei als sauber oder infiziert erkannt wird, wird diese Information an den Computer gesendet und der Status der Datei wird aktualisiert.

- **Beispieldatei senden:** Kann eine als verdächtig eingestufte Datei nicht alleine anhand der Dateiinformationen als schädlich identifiziert werden, können Sie Sophos erlauben, das Senden einer Beispieldatei anzufordern. Wenn diese Option aktiviert ist und Sophos nicht bereits über ein Muster dieser Datei verfügt, wird die betreffende Datei automatisch gesendet. Durch das Einsenden von Beispieldateien kann Sophos die Schadsoftware-Erkennung kontinuierlich verbessern und Fehlfunde vermeiden.

Verdächtiges Verhalten (HIPS): Aktivieren Sie diese Option, um alle Systemprozesse auf Zeichen aktiver Schadsoftware hin zu überwachen. Dazu gehören verdächtige Einträge in das Registry, Dateikopiervorgänge oder Pufferüberlauf-Techniken. Verdächtige Prozesse werden blockiert.

Web Protection: Aktivieren Sie diese Option, um Website-URLs in der Online-Datenbank der infizierten Websites von Sophos nachzuschlagen.

- **Websites mit schädlichen Inhalten blockieren:** Aktivieren Sie diese Option, um Websites mit schädlichen Inhalten zu blockieren.

- **Download-Scan:** Aktivieren Sie diese Option, um Daten während des Herunterladens nach Viren zu scannen. Infizierte Dateien werden blockiert.

Geplanter Scan: Aktivieren Sie diese Option, um den Scan zu einem bestimmten Zeitpunkt auszuführen.

- **Rootkit-Scan:** Aktivieren Sie diese Option, um bei jedem geplanten Scan den Computer nach Rootkits zu durchsuchen.
- **Scan mit niedriger Priorität:** Aktivieren Sie diese Option, um On-Demand-Scans mit einer niedrigeren Priorität durchzuführen. Beachten Sie, dass dies erst ab Windows Vista Servicepack 2 möglich ist.
- **Zeit-Ereignis:** Geben Sie hier an, wann der Computer gescannt werden soll. Beachten Sie dabei die Zeitzone des Endpoints.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
Die neue Richtlinie wird in der Liste der Antiviren-Richtlinien angezeigt. Beachten Sie, dass Änderungen an den Einstellungen erst nach 15 Minuten auf allen Computern wirksam werden.

Um eine Richtlinie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

11.2.2 Ausnahmen

Auf der Registerkarte *Endpoint Protection* > *Antivirus* > *Ausnahmen* können Sie einzelne Computergruppen von den Antivirus-Einstellungen des Endpoint-Protection-Moduls ausnehmen. Eine Ausnahme legt fest, welche Objekte von dem in einer Antiviren-Richtlinieneinstellung definierten Scanvorgang ausgenommen werden.

Um eine Ausnahme hinzuzufügen, gehen Sie folgendermaßen vor:

Klicken Sie auf der Registerkarte *Ausnahmen* auf *Ausnahme hinzufügen*.
1. Das Dialogfeld *Ausnahme hinzufügen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Typ: Wählen Sie den Typ der Objekte aus, die vom Zugriffs- und On-Demand-Scan ausgenommen sein sollen.

   - **Adware und PUA:** Wählen Sie diese Option, wenn bestimmte Adware oder PUA (Potenziell Unerwünschte Anwendungen) nicht gescannt oder blockiert werden soll. Adware zeigt unerwünschte Werbung an (zum Beispiel in Pop-up-Fenstern)

und kann die Benutzerproduktivität und Systemeffizienz beeinträchtigen. PUAs richten keinen Schaden an, haben aber in geschäftlich genutzten Netzwerken nichts zu suchen. Geben Sie unter *Dateiname* den Namen der Adware oder PUA ein, z. B. `beispiel.zeug`.

- **Scan-Ausnahmen:** Wählen Sie diese Option, um eine Datei, einen Ordner oder ein Netzlaufwerk vom Antiviren-Scan auszuschließen. Unter *Datei/Pfad* geben Sie eine Datei, einen Ordner oder ein Netzlaufwerk an, z. B. `C:\Dokumente\` oder `\\Server\Benutzer\Dokumente\Lebenslauf.doc`.
- **Scan-Erweiterungen:** Wenn diese Option ausgewählt ist, können Sie Dateien mit einer bestimmten Erweiterung hinzufügen, damit sie von einem Antivirenscan durchsucht werden.Geben Sie die Erweiterung in das Feld *Erweiterung* ein, z. B. `html`.
- **Pufferüberlauf:** Wählen Sie diese Option, um zu verhindern, dass die Verhaltensüberwachung Anwendungen blockiert, die Pufferüberlauf-Techniken nutzen. Geben Sie optional den Namen der Anwendungsdatei in das Feld *Dateiname* ein und laden Sie die Datei über das Feld *Hochladen* hoch.
- **Verdächtige Dateien:** Wählen Sie diese Option, um zu verhindern, dass der Antiviren-Scan verdächtige Dateien blockiert. Laden Sie die Datei über das Feld *Hochladen* hoch.UTMgeneriert die MD5-Prüfsumme der Datei. Der Name der hochgeladenen Datei wird automatisch für das Feld *Dateiname* verwendet. Ändern Sie optional den Dateinamen. Wenn eine Datei mit dem festgelegten Dateinamen und der gespeicherten MD5-Prüfsumme auf dem Client gefunden wird, wird sie nicht durch Antiviren-Scanning blockiert.
- **Verdächtiges Verhalten:** Wählen Sie diese Option, um zu verhindern, dass eine Datei von der Verhaltensüberwachung blockiert wird. Geben Sie optional den Namen der Datei in das Feld *Dateiname* ein und laden Sie die Datei über das Feld *Hochladen* hoch.
- **Websites:** Wählen Sie diese Option, um Websites, die den Attributen im Feld *Webformat* entsprechen, vom Antivirenscan auszunehmen.
  Webformat: Geben Sie hier die Server mit den Websites an, deren Besuch zulässig sein soll.
  - **Domänenname:** Geben Sie in das Feld *Website* den Namen der Domäne ein, die Sie zulassen möchten.
  - **IP-Adresse mit Subnetzmaske:** Geben Sie hier die IPv4-Adresse und die Netzmaske der Computer ein, die Sie zulassen möchten.

- **IP-Adresse:** Geben Sie hier die IPv4-Adresse des Computers ein, den Sie zulassen möchten.

Hochladen (Nur verfügbar bei den Typen *Pufferüberlauf*, *Verdächtige Dateien* und *Verdächtiges Verhalten*): Laden Sie hier die Datei hoch, die vom Antiviren-Scan ausgenommen sein soll.

Computergruppen: Wählen Sie die Computergruppen aus, für die diese Ausnahme gelten soll.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

11.3 Device Control

Auf den Seiten *Endpoint Protection > Device Control* können Sie Geräte kontrollieren, die an die Computer, die mit Endpoint Protection überwacht werden, angeschlossen sind. In einer Geräterichtlinie legen Sie im Prinzip fest, welche Gerätetypen für die Computergruppen, denen die Richtlinie zugewiesen ist, zulässig sind oder blockiert werden. Sobald ein Gerät gefunden wird, prüft Endpoint Protection, ob es gemäß der Geräterichtlinie, die der Computergruppe des betreffenden Computers zugewiesen ist, zulässig ist. Wenn es laut Geräterichtlinie blockiert oder eingeschränkt ist, wird es auf der Registerkarte *Ausnahmen* angezeigt, auf der Sie eine Ausnahme für das Gerät hinzufügen können.

11.3.1 Richtlinien

Auf der Registerkarte *Endpoint Protection > Device Control > Richtlinien* können Sie verschiedene zusammengefasste Einstellungen für Device Control verwalten, die daraufhin auf die von Endpoint Protection überwachten Computergruppen angewandt werden können. Diese zusammengefassten Einstellungen werden als Richtlinien bezeichnet.

Standardmäßig stehen zwei Geräterichtlinien zur Verfügung: *Alle blockieren* verbietet jegliche Nutzung von Geräten, während *Vollständiger Zugriff* alle Berechtigungen für sämtliche Geräte zulässt. Diese Richtlinien können nicht geändert werden.

Um eine neue Richtlinie hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Richtlinie hinzufügen*.**
   Das Dialogfeld *Richtlinie hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Richtlinie ein.

   Speichergeräte: Sie können für verschiedene Arten von Speichergeräten konfigurieren, ob sie *Zugelassen* oder *Blockiert* sein sollen.Gegebenenfalls ist auch der Eintrag *Lesezugriff* verfügbar.

   Netzwerkgeräte: Sie können für Modems und WLAN-Netzwerke konfigurieren, ob sie *Zugelassen*, *Bei Bridging blockiert* oder *Blockiert* sein sollen.

   Short Range Devices: Sie können für Bluetooth- und Infrarotgeräte konfigurieren, ob sie *Zugelassen* oder *Blockiert* sein sollen.

3. **Kommentar** (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

4. **Klicken Sie auf *Speichern*.**
   Die neue Richtlinie wird in der Liste der Device-Control-Richtlinien angezeigt. Sie kann nun auf eine Computergruppe angewendet werden. Beachten Sie, dass Änderungen an den Einstellungen erst nach 15 Minuten auf allen Computern wirksam werden.

Um eine Richtlinie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

11.3.2 Ausnahmen

Auf der Registerkarte *Endpoint Protection > Device Control > Ausnahmen* können Sie für bestimmte Geräte Schutzausnahmen festlegen. Durch eine Ausnahme wird etwas zugelassen, das laut Geräterichtlinie, die einer Computergruppe zugewiesen ist, verboten ist. Ausnahmen werden für Computergruppen angelegt, daher gilt eine Ausnahme immer für alle Computer der gewählten Gruppe(n).

Die Liste *Ausnahmen* zeigt automatisch alle erkannten Geräte, die durch die angewendeten Device-Control-Richtlinien blockiert sind oder auf die nur eingeschränkt zugegriffen werden kann. Wenn mehrere Diskettenlaufwerke angeschlossen sind, wird, da Diskettenlaufwerke technisch nicht unterschieden werden können, nur ein Eintrag angezeigt, welcher alle Diskettenlaufwerke repräsentiert.

Um für ein Gerät eine Ausnahme hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Bearbeiten* eines Gerätes.**
   Das Dialogfeld *Gerät bearbeiten* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Zugelassen: Fügen Sie die Computergruppen hinzu, für die das Gerät zugelassen sein soll.

   Lesezugriff oder gebridged: Fügen Sie die Computergruppen hinzu, für die dieses Gerät nur mit Lesezugriff (gilt für Speichergeräte) oder im Modus „Bridged“ (gilt für Netzwerkgeräte) zugelassen sein soll.

   Auf alle anwenden: Ist diese Option ausgewählt, werden die aktuellen Einstellungen auf alle Geräte mit der gleichen Geräte-ID angewendet. Dies ist beispielsweise dann hilfreich, wenn Sie die gleiche, generische Ausnahme auf mehrere USB-Sticks des gleichen Typs anwenden wollen.

   Modus: Diese Option ist nur verfügbar, wenn Sie das Auswahlkästchen *Auf alle anwenden* deaktivieren. In diesem Fall müssen Sie festlegen, was mit anderen Geräten geschehen soll, die über die gleiche generische Ausnahme verfügen. Wenn Sie die generische Ausnahme für die betreffenden Geräte beibehalten möchten, wählen Sie *Für andere beibehalten*. Wenn Sie die generische Ausnahme löschen möchten, wählen Sie *Für andere löschen*.

   Tipp – Weitere Informationen und Beispiele zu generischen Ausnahmen finden Sie im Abschnitt Mit generellen Ausnahmen arbeiten unten.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**

   Die Computergruppen und ihre Ausnahmen werden mit dem bearbeiteten Gerät angezeigt.

Hinweis – Sobald ein Gerät auf der Liste *Ausnahmen* aufgeführt wird, bleibt es so lange auf dieser Liste, bis Sie es mit der Schaltfläche *Löschen* entfernen. Typischerweise würden Sie ein Gerät löschen, nachdem die entsprechende Hardware endgültig entfernt wurde (z. B.: ein CD-Laufwerk existiert nicht mehr) oder nachdem Sie Ihre Device-Richtlinien geändert haben (z. B.: WLAN-Netzwerkadapter sind jetzt generell erlaubt). Wenn Sie ein Gerät löschen, das noch verwendet wird, wird eine Meldung angezeigt, die Sie mit *OK* bestätigen müssen.

Anschließend wird das Gerät von der Liste gelöscht. Wenn für dieses Gerät eine Ausnahme besteht, wird diese automatisch ungültig, d. h. die aktuelle Device-Richtlinie wird auf das Gerät angewendet.

Mit generischen Ausnahmen arbeiten

Eine generische Device-Ausnahme ist eine Ausnahme, die automatisch allen Geräten zugeordnet wird, die die gleiche Geräte-ID besitzen.

Generische Ausnahme anlegen

1. Klicken Sie auf die Schaltfläche *Bearbeiten* eines Gerätes, das über keine generische Ausnahme verfügt, d. h. dessen Auswahlkästchen *Auf alle anwenden* nicht ausgewählt ist.
2. Definieren Sie die Ausnahme und aktivieren Sie das Auswahlkästchen *Auf alle anwenden*.
3. Speichern Sie die Ausnahme.
   Die Ausnahme wird auf alle Geräte angewendet, die dieselbe Geräte-ID besitzen.

Gerät von einer generischen Ausnahme ausschließen

1. Klicken Sie auf die Schaltfläche *Bearbeiten* des Gerätes, das Sie von einer vorhandenen generischen Ausnahme ausschließen möchten.
2. Definieren Sie die individuelle Ausnahme und deaktivieren Sie das Auswahlkästchen *Auf alle anwenden*.
3. Wählen Sie in der Auswahlliste *Modus* den Eintrag *Für andere beibehalten*.
4. Speichern Sie die Ausnahme.
   Das bearbeitete Gerät verfügt jetzt über eine individuelle Ausnahme, während die anderen Geräte weiterhin über die generische Ausnahme verfügen.

Einstellungen für alle Geräte einer generischen Ausnahme ändern

1. Klicken Sie auf die Schaltfläche *Bearbeiten* eines der Geräte mit der generischen Ausnahme.
2. Bearbeiten Sie die Ausnahme und lassen Sie das Auswahlkästchen *Auf alle anwenden* ausgewählt.

3. Speichern Sie die Ausnahme.
   Die Einstellungen aller Geräte mit derselben Geräte-ID, bei denen das Auswahlkästchen *Auf alle anwenden* ausgewählt ist, werden entsprechend geändert.

Generische Ausnahme löschen

1. Klicken Sie auf die Schaltfläche *Bearbeiten* eines der Geräte mit der generischen Ausnahme.
2. Deaktivieren Sie das Auswahlkästchen *Auf alle anwenden*.
3. Wählen Sie in der Auswahlliste *Modus* den Eintrag *Für andere löschen*.
4. Speichern Sie die Ausnahme.
   Die Ausnahmen aller Geräte mit derselben Geräte-ID, bei denen das Auswahlkästchen *Auf alle anwenden* ausgewählt war, werden gelöscht. Nur das bearbeitete Gerät besitzt noch eine, jetzt individuelle, Ausnahme.

11.4 Endpoint Web Control

Während Sophos UTM Sicherheit und Produktivitätsschutz für Systeme bietet, die vom Unternehmensnetzwerk aus im Internet surfen, dehnt Endpoint Web Control diesen Schutz auf die Computer der Benutzer aus. Es bietet Schutz, Kontrolle und Berichtsfunktionen für Endpoint-Computer, die sich außerhalb Ihres Unternehmensnetzwerks befinden. Wenn Endpoint Web Control aktiv ist, werden alle Richtlinien, die unter *Web Protection* > *Webfilter* und *Web Protection* > *Webfilter-Profile* > *Proxy-Profile* festgelegt sind, durchgesetzt, selbst wenn sich der Computer nicht in einem UTM-Netzwerk befindet. Sophos UTMund Sophos-Endpoints kommunizieren über LiveConnect, einen Cloud-Dienst, der Richtlinien und Berichtsdaten ständig aktuell hält, indem er Sophos UTM und mobile Sophos-Endpoints nahtlos verbindet. Ein Laptop setzt beispielsweise auch zu Hause oder in einem Café die Web-Control-Richtlinien um und Sophos UTM erhält Protokollinformationen vom mobil eingesetzten Laptop.

11.4.1 Allgemein

Auf der Registerkarte *Endpoint Protection* > *Web Control* > *Allgemein* können Sie Endpoint Web Control aktivieren oder deaktivieren. Um Filterrichtlinien für Endpoint Web Control zu konfigurieren, müssen Sie Web Control für die entsprechende Computergruppe auf der Seite *Endpoint Protection* > *Computerverwaltung* > *Gruppen verwalten* aktivieren und die Gruppe auf

der Registerkarte *Web Protection* > *Webfilter-Profile* > *Proxy-Profile* in einem Proxy-Profil auswählen.

11.4.2 Erweitert

Auf der Registerkarte *Endpoint Protection* > *Web Control* > *Erweitert* können Sie *Verkehr auf Gateway und auf Endpoint scannen auswählen* . Standardmäßig scannt Sophos UTM Internetverkehr nicht für Endpoints, auf denen Web Control aktiv ist. Wenn diese Option ausgewählt ist, filtern sowohl der Endpoint als auch Sophos UTM den Internetverkehr. Um die Sicherheit zu erhöhen, wählen Sie auf *Web Protection* > *Webfilter* > *Richtlinien* > *Antivirus* die Einstellung *Zweifachscan (max. Sicherheit)*,oder wählen Sie alternativ auf der Registerkarte *Verwaltung* > *Systemeinstellungen* > *Scan-Einstellungen* einen anderen Virenerkennungsmechanismus. Durch beide Möglichkeiten wird auf Sophos UTM ein anderer Antiviren-Mechanismus verwendet als auf dem Endpoint, was die Sicherheit erhöht.

11.4.3 Nicht unterstützte Funktionen

Obwohl es viele Vorteil hat, Web Control auf den Endpoint auszudehnen, stehen einige Funktionen dennoch nur von einem Sophos UTM-Netzwerk aus zur Verfügung. Die folgenden Funktionen werden zwar von Sophos UTM, jedoch nicht von Endpoint Web Control unterstützt:

- **HTTPS-Verkehr (SSL) scannen:** HTTPS-Verkehr kann nicht vom Endpoint gescannt werden. Wenn der Endpoint UTM als Proxy verwendet und diese Funktion aktiv ist, wird der Verkehr durch UTM gescannt.
- **Authentifizierungsmodus:** Der Endpoint verwendet immer den aktuell eingeloggten Benutzer (SSO). Der Endpoint kann keine Authentifizierung durchführen, da er, wenn er mobil verwendet wird, nicht in der Lage ist, zum Zwecke der Authentifizierung mit UTM zu kommunizieren.
- **Antivirus/Schadsoftware:** Sophos Endpoint-Antiviruseinstellungen werden auf der Seite *Endpoint Protection* > *Antivirus* festgelegt. Wenn Web Protection (Download-Scanning) eingeschaltet ist, führt es für das gesamte Internetangebot immer einen Antiviren-Einzelscan durch. Zweifachscan und maximale Scangröße werden nicht unterstützt.
- **Entfernen von aktivem Inhalt**
- **YouTube für Schulen**
- **Streaming-Einstellungen:** Der Sophos-Endpoint scannt Streaming-Inhalte immer auf Viren.

- **Unscannbare und verschlüsselte Dateien blockieren**
- **Nach Download-Größe blockieren**
- **Zugelassene Zieldienste:** Diese Funktion steht nur auf Sophos UTM zur Verfügung.
- **Webfilter-Zwischenspeicherung:** Diese Funktion steht nur auf Sophos UTM zur Verfügung.

12 Wireless Protection

Über das Menü *Wireless Protection* können Sie WLAN-Access-Points für Sophos UTM, die zugehörigen WLAN-Netzwerke und die Clients, die WLAN-Zugang nutzen, konfigurieren und verwalten. Die Access Points werden automatisch auf UTM konfiguriert, Sie müssen sie also nicht einzeln konfigurieren. Die Kommunikation zwischen UTM und dem Access Point, die der Konfiguration des Access Points sowie dem Austausch von Statusinformationen dient, wird mittels AES verschlüsselt.

Wichtiger Hinweis – Wenn die Lichter an Ihrem Access Point schnell blinken, trennen Sie ihn nicht vom Strom! Schnell blinkende Lichter bedeuten, dass gerade ein Firmware-Flash durchgeführt wird. Ein Firmware-Flash erfolgt beispielsweise nach einer Systemaktualisierung von UTM, die mit einer Aktualisierung von Wireless Protection einhergeht.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Allgemein
- WLAN-Netzwerke
- Mesh-Netzwerke
- Access Points
- WLAN-Clients
- Hotspots

Die Übersichtsseite von Wireless Protection bietet allgemeine Informationen zu verbundenen Access Points, deren Status, verbundenen Clients, WLAN-Netzwerken, Mesh-Netzwerken und Mesh-Peer-Links.

Im Bereich *Momentan verbunden* können Sie die Einträge nach SSID oder Access Point sortieren, und Sie können einzelne Einträge mit Hilfe des Reduzieren-Symbols aus- und einklappen.

Live-Protokoll

Sie können auf die Schaltfläche *Wireless-Protection-Live-Protokoll öffnen* klicken, um detaillierte Verbindungs- und Fehlersuche-Informationen über die Access Points und Clients zu erhalten, die versuchen, eine Verbindung herzustellen.

12.1 Allgemein

Auf den Seiten *Wireless Protection > Allgemeine Einstellungen* können Sie Wireless Protection aktivieren und die Netzwerkschnittstellen für Wireless Protection sowie die WPA/WPA2-Enterprise-Authentifizierung konfigurieren.

12.1.1 Allgemein

Auf der Registerkarte *Wireless Protection > Allgemeine Einstellungen > Allgemein* können Sie Wireless Protection aktivieren oder deaktivieren.

Um Wireless Protection zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Wireless Protection auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Zugangskontrolle* kann bearbeitet werden.

   Bei der erstmaligen Aktivierung von Wireless Protection wird der Abschnitt *Ersteinrichtung* angezeigt. Dieser Abschnitt enthält die Konfiguration, die erzeugt wird: ein eigenständiges WLAN-„Gast"-Netzwerk mit WPA2-Personal-Verschlüsselung und DHCP für WLAN-Clients. Die WLAN-Clients können DNS auf UTM und den *Web-Surfing*-Dienst verwenden. Der vorverteilte Schlüssel wird automatisch generiert und nur in diesem Abschnitt angezeigt. Diese Erstkonfiguration soll als Vorlage dienen. Sie können die Einstellungen jederzeit auf der Seite *Wireless Protection > WLAN-Netzwerke* bearbeiten.

   Automatische Konfiguration nicht durchführen: Wählen Sie diese Option, wenn keine Ersteinrichtung durchgeführt werden soll. Dann müssen Sie die Einstellungen für Wireless Protection manuell durchführen.

2. **Wählen Sie eine Netzwerkschnittstelle für den Access Point.**
   Klicken Sie auf das Ordnersymbol im Abschnitt *Zugelassene Schnittstellen*, um eine konfigurierte Schnittstelle auszuwählen, an die der Access Point angeschlossen wird. Stellen Sie sicher, dass die Schnittstelle von einem DHCP-Server verwaltet wird.

3. **Klicken Sie auf *Übernehmen*.**

   Ihre Einstellungen werden gespeichert. Der Schieberegler wird grün und zeigt dadurch an, dass Wireless Protection aktiv ist.

Sie können nun fortfahren, indem Sie den Access Point an die konfigurierte Netzwerkschnittstelle anschließen. Wenn Sie die automatische Konfiguration übersprungen haben, fahren Sie mit der Konfiguration auf der Seite *WLAN-Netzwerke* fort.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

Sobald Sie einen Access Point anschließen, wird er sich automatisch mit dem System verbinden. Neu angeschlossene, unkonfigurierte Access Points werden auf der Seite *Access Points* > *Übersicht* als *Ausstehende Access Points* angezeigt.

12.1.2 Erweitert

Auf der Registerkarte *Wireless Protection* > *Allgemeine Einstellungen* > *Erweitert* können Sie Ihre Access Points so konfigurieren, dass sie WPA/WPA2-Enterprise-Authentifizierung verwenden.

Die Enterprise-Authentifizierung erfordert einige Angaben zu Ihrem RADIUS-Server. Beachten Sie, dass die APs nicht selbst mit dem RADIUS-Server für die Authentifizierung kommunizieren, sondern nur UTM.Port `414` wird für die RADIUS-Kommunikation zwischen UTM und dem/den AP(s) verwendet.

Um WPA/WPA2-Enterprise-Authentifizierung zu verwenden, nehmen Sie die folgenden Einstellungen vor:

RADIUS-Server: Wählen Sie einen Server (oder legen Sie einen an), über den sich Clients selbst authentifizieren sollen, z. B. Ihren Active-Directory-Server.

RADIUS-Port (optional): Der RADIUS-Standardport 1812 ist vorausgewählt. Falls notwendig, können Sie diesen Port ändern.

RADIUS-Kennwort: Geben Sie das RADIUS-Kennwort ein, das von den Access Points benötigt wird, um mit dem RADIUS-Server kommunizieren zu können.

Testeinstellungen: Klicken Sie, um zu überprüfen, ob die Verbindung zum RADIUS-Server erfolgreich hergestellt werden kann.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

12.2 WLAN-Netzwerke

Auf der Seite *Wireless Protection > WLAN-Netzwerke* können Sie Ihre WLAN-Netzwerke definieren, z. B. ihre SSID und Verschlüsselungsmethode. Darüber hinaus können Sie festlegen, ob das WLAN-Netzwerk einen eigenständigen IP-Adressbereich oder eine Bridge in das LAN des Access Points haben soll.

Um ein neues WLAN-Netzwerk anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *WLAN-Netzwerke* auf *WLAN-Netzwerk hinzufügen*.**
   Das Dialogfeld *WLAN-Netzwerk hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Netzwerkname: Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.

   Netzwerk-SSID: Geben Sie den Service Set Identifier (SSID) für das Netzwerk ein, der von den Clients registriert wird und zur Identifizierung des kabellosen Netzwerks dient. Die SSID kann aus 1 bis 32 druckbaren ASCII-Zeichen bestehen[1]. Sie darf kein Komma enthalten und nicht mit einem Leerzeichen beginnen oder enden.

   Verschlüsselungsmethode: Wählen Sie eine Verschlüsselungsmethode aus der Auswahlliste. Standardmäßig ist *WPA 2 Personal* eingestellt. Wir empfehlen *WPA2* statt *WPA*, wenn möglich. Aus Sicherheitsgründen wird davon abgeraten, WEP zu verwenden, es sei denn, Ihr WLAN-Netzwerk wird von Clients genutzt, die keine andere Methode unterstützen. Wenn Sie eine Enterprise-Authentifizierungsmethode verwenden, müssen Sie auch einen RADIUS-Server auf der Registerkarte *Allgemeine Einstellungen > Erweitert* konfigurieren. Geben Sie als NAS-ID des RADIUS-Servers den Namen des WLAN-Netzwerks ein.

   Kennwort/PSK: Nur verfügbar bei der Verschlüsselungsmethode *WPA/WPA2 Personal*. Geben Sie das Kennwort ein, das das WLAN-Netzwerk vor unautorisiertem Zugriff schützen soll und wiederholen Sie es im nächsten Feld. Das Kennwort darf aus 8 bis 63 druckbaren ASCII-Zeichen bestehen.

[1] http://de.wikipedia.org/wiki/ASCII#ASCII_printable_characters

128-Bit WEP-Schlüssel: Nur verfügbar bei der Verschlüsselungsmethode *WEP*. Geben Sie hier einen WEP-Schlüssel ein, der aus genau 26 hexadezimalen Zeichen besteht.

Client-Verkehr: Wählen Sie eine Methode, wie Ihr kabelloses Netzwerk in Ihr lokales Netzwerk integriert werden soll.

- **Getrennte Zone** (Standard): Das kabellose Netzwerk wird als eigenständige Zone behandelt und hat einen eigenen IP-Adressbereich. Wenn Sie diese Option nutzen, müssen Sie, nachdem Sie das WLAN-Netzwerk hinzugefügt haben, mit der Einrichtung wie im Abschnitt unten (Nächste Schritte für Netzwerke in getrennter Zone) beschrieben fortfahren.

  Hinweis – Wenn Sie ein Netzwerk der Art *Getrennte Zone* zu einem Netzwerk der Art *In AP-LAN bridgen* oder *In VLAN bridgen* ändern, werden bereits konfigurierte WLAN-Schnittstellen auf UTM deaktiviert und das Schnittstellenobjekt erhält den Status *nicht zugewiesen*. Sie können dem Schnittstellenobjekt jedoch eine neue Hardware-Schnittstelle zuweisen, indem Sie es bearbeiten und dadurch wieder aktivieren.

- **In AP-LAN bridgen:** Sie können das kabellose Netzwerk auch in das Netzwerk des Access Point bridgen. Das heißt, dass die WLAN-Clients einen gemeinsamen IP-Adressbereich besitzen.

  Hinweis – Wenn VLAN aktiviert ist, werden die WLAN-Clients in das VLAN-Netzwerk des Access Points gebridged.

- **In VLAN bridgen:** Sie können den Verkehr dieses kabellosen Netzwerks in ein VLAN Ihrer Wahl bridgen. Das ist nützlich, wenn Sie wollen, dass die Access Points in einem gemeinsamen Netzwerk getrennt von den WLAN-Clients sind.
  In VLAN-ID bridgen: Geben Sie die VLAN-ID des Netzwerks ein, zu dem die WLAN-Clients gehören sollen.

  Client-VLAN-ID (nur mit einer *Enterprise*-Verschlüsselungsmethode verfügbar): Wählen Sie, wie die VLAN-ID definiert ist:

  - **Statisch:** Die VLAN-ID, die im Feld *In VLAN-ID bridgen* definiert ist, wird verwendet.

- **RADIUS & Statisch:** Die VLAN-ID Ihres RADIUS-Servers wird verwendet: Wenn ein Benutzer eine Verbindung mit einem Ihrer kabellosen Netzwerke herstellt und sich an Ihrem RADIUS-Server authentifiziert, teilt der RADIUS-Server dem Access Point mit, welche VLAN-ID für diesen Benutzer verwendet werden soll. Wenn Sie mehrere WLAN-Netzwerke verwenden, können Sie den Zugriff auf interne Netzwerke daher nach Benutzer festlegen. Wenn einem Benutzer kein VLAN-ID-Attribut zugewiesen wurde, wird die VLAN-ID, die im Feld *In VLAN-ID bridgen* definiert ist, verwendet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
Algorithmus (nur verfügbar bei der Verschlüsselungsmethode WPA/WPA2): Wählen Sie einen Verschlüsselungsalgorithmus: entweder *AES* oder *TKIP & AES*.Aus Sicherheitsgründen empfehlen wir, *AES* zu verwenden.

Frequenzband: Die Access Points, die diesem WLAN-Netzwerk zugewiesen sind, werden auf dem ausgewählten Frequenzband übertragen. Das 5-GHz-Band weist im Allgemeinen eine höhere Leistung, eine geringere Latenz und weniger Störungen auf. Daher sollte es z. B. bei VoIP-Kommunikation gewählt werden. Beachten Sie, dass nur AP 50 auf dem 5-GHz-Band senden kann.

Zeitbasierter Zugriff: Wählen Sie diese Option, wenn Sie das kabellose Netzwerk automatisch gemäß eines Zeitplans aktivieren und deaktivieren möchten.

Aktive Zeit auswählen: Wählen Sie eine Zeitraumdefinition, die festlegt, wann das kabellose Netzwerk aktiv ist. Sie können eine neue Zeitraumdefinition hinzufügen, indem Sie auf das Plussymbol klicken.

Client-Isolation: Clients innerhalb eines Netzwerks können normalerweise miteinander kommunizieren. Wenn Sie das verhindern wollen, beispielsweise in einem Gastnetzwerk, wählen Sie *Aktiviert* aus der Auswahlliste.

SSID verstecken: Manchmal möchten Sie Ihre SSID nicht anzeigen. Wählen Sie dazu *Ja* aus der Auswahlliste. Bitte beachten Sie, dass es sich hierbei nicht um eine Sicherheitsfunktion handelt.

MAC-Filter-Typ: Um die MAC-Adressen einzuschränken, die sich mit diesem WLAN-Netzwerk verbinden dürfen, wählen Sie *Blacklist* oder *Whitelist*. Mit *Blacklist* sind

alle MAC-Adressen erlaubt, außer denen, die auf der unten ausgewählten MAC-Adressliste stehen. Mit *Whitelist* sind alle MAC-Adressen verboten, außer denen, die auf der unten ausgewählten MAC-Adressliste stehen.

MAC-Adressen: Die Liste der MAC-Adressen, die für die Beschränkung des WLAN-Netzwerks verwendet wird. MAC-Adresslisten können auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen > MAC-Adressdefinitionen* erstellt werden. Hinweis: Es sind maximal 200 MAC-Adressen zulässig.

4. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert.Das WLAN-Netzwerk wird in der Liste *WLAN-Netzwerke* angezeigt.

Nächste Schritte für Netzwerke in getrennter Zone

Wenn Sie ein WLAN-Netzwerk mit der Option *Getrennte Zone* erstellen, wird automatisch eine entsprechende neue virtuelle Hardwareschnittstelle erstellt, z. B. *wlan0*. Um das WLAN-Netzwerk nutzen zu können, sind einige weitere manuelle Konfigurationen erforderlich. Gehen Sie folgendermaßen vor:

1. **Konfigurieren Sie eine neue Netzwerkschnittstelle.**
   Erstellen Sie auf der Registerkarte *Schnittstellen & Routing > Schnittstellen > Schnittstellen* eine neue Schnittstelle und wählen Sie Ihre WLAN-Schnittstelle (z. B. wlan0) als Hardware. Stellen Sie sicher, dass Sie „Ethernet“ als Art gewählt haben und geben Sie die IP-Adresse und Netzmaske Ihres WLAN-Netzwerks an.

2. **Aktivieren Sie DHCP für die WLAN-Clients.**
   Damit Ihre Clients eine Verbindung zu UTM herstellen können, müssen Sie ihnen eine IP-Adresse und ein Standardgateway zuweisen. Richten Sie hierzu auf der Registerkarte *Netzwerkdienste > DHCP > Server* einen DHCP-Server für die Schnittstelle ein.

3. **Aktivieren Sie DNS für die WLAN-Clients.**
   Damit Ihre Clients DNS-Namen auflösen können, benötigen Sie Zugriff auf DNS-Server. Fügen Sie auf der Registerkarte *Netzwerkdienste > DNS > Allgemein* die Schnittstelle zur Liste der zugelassenen Netzwerke hinzu.

4. **Erstellen Sie eine NAT-Regel, um das WLAN-Netzwerk zu maskieren.**

Wie bei jedem anderen Netzwerk müssen Sie auch hier die Adressen des WLAN-Netzwerks in die Adresse der Uplink-Schnittstelle übersetzen. Erstellen Sie eine NAT-Regel auf der Registerkarte *Network Protection > NAT > Maskierung*.

5. **Erstellen Sie eine oder mehrere Paketfilterregeln, um Verkehr vom WLAN-Netzwerk bzw. dorthin zuzulassen.**
   Wie bei jedem anderen Netzwerk müssen Sie auch hier eine oder mehrere Paketfilterregeln erstellen, damit der Verkehr UTM passieren kann, z. B. Web-Surfing-Verkehr. Paketfilterregeln erstellen Sie auf der Registerkarte *Network Protection > Firewall > Regeln*.

12.3 Access Points

Die Seiten *Wireless Protection > Access Points* geben einen Überblick über die Access Points (AP), die dem System bekannt sind. Sie können AP-Eigenschaften bearbeiten, APs löschen oder gruppieren und APs oder AP-Gruppen WLAN-Netzwerke zuweisen.

Hinweis – Mit dem BasicGuard-Abonnement kann nur ein Access Point mit der UTM verbunden sein. Für alle UTM-Appliances ist die Anzahl an Access Points auf maximal 223 begrenzt.

Arten von Access Points

Momentan bietet Sophos vier verschiedene Access Points an:

- AP 5: Standards 802.11b/g/n, Frequenzband 2,4 GHz
  Er kann nur mit einem RED Rev2 oder Rev3 mit USB-Anschluss verbunden werden und unterstützt genau eine SSID mit WLAN-Typ *In AP-LAN bridgen* und maximal 7 WLAN-Clients.
- AP 10: Standards 802.11b/g/n, Frequenzband 2,4 GHz
- AP 30: Standards 802.11b/g/n, Frequenzband 2,4 GHz
- AP 50: Standards 802.11a/b/g/n, Frequenzbänder 2,4/5 GHz Dualband/Dualfunk
  Es gibt zwei verschiedene AP-50-Modelle, bei denen sich die verfügbaren Kanäle unterscheiden.
  - FCC-regulierte Gebiete (hauptsächlich USA): Kanäle 1–11, 36, 40, 44, 48
  - ETSI-regulierte Gebiete (hauptsächlich Europa): Kanäle 1–13, 36, 40, 44, 48

Beachten Sie, dass die Ländereinstellung eines AP reguliert, welche Kanäle zur Verfügung stehen, um der Gesetzeslage vor Ort zu entsprechen.

Querverweis – Detaillierte Informationen über Access Points finden Sie in den *Hinweisen zum Betrieb* im Sophos UTM-Resource-Center.

12.3.1 Übersicht

Die Seite *Wireless Protection > Access Points > Übersicht* liefert einen Überblick über die Access Points (APs), die dem System bekannt sind.Die Sophos UTM unterscheidet zwischen aktiven, inaktiven und ausstehenden APs.Um sicherzustellen, dass sich nur originale APs mit Ihrem Netzwerk verbinden, müssen die APs zunächst autorisiert werden.

Hinweis – Wenn Sie vorhaben, einen AP 5 zu verwenden, müssen Sie zuerst die RED-Verwaltung aktivieren und ein RED einrichten. Fügen Sie die RED-Schnittstelle anschließend auf der Seite *Wireless Protection > Allgemeine Einstellungen* zur Liste der zugelassenen Schnittstellen hinzu. Nachdem Sie den AP 5 mit dem RED verbunden haben, sollte der AP 5 unter *Ausstehende Access Points* angezeigt werden.

Access Points können auf der Registerkarte *Gruppierung* zeitweise deaktiviert werden.Wenn ein AP physikalisch von Ihrem Netzwerk getrennt wird, können Sie ihn hier durch einen Klick auf die Schaltfläche *Löschen*entfernen. Solange der AP mit Ihrem Netzwerk verbunden bleibt, wird er nach dem Löschen automatisch wieder mit dem Status *Ausstehend* angezeigt.

Tipp – Jeder Abschnitt auf dieser Seite kann mit Hilfe des Reduzieren-Symbols rechts neben der Kopfzeile des Abschnitts auf- und zugeklappt werden.

Aktive Access Points

Hier werden alle APs aufgeführt, die verbunden, konfiguriert und momentan in Betrieb sind.Um einen AP zu bearbeiten, klicken Sie auf die Schaltfläche *Bearbeiten* (siehe *Einen Access Point bearbeiten* unten).

Inaktive Access Points

Hier werden alle APs aufgeführt, die bereits einmal konfiguriert wurden, aber momentan nicht mit der UTM verbunden sind. Wenn ein AP länger als fünf Minuten in diesem Status bleibt, überprüfen Sie bitte die Netzwerkverbindung des AP und Ihre Systemkonfiguration. Bei einem

Neustart des Dienstes Wireless Protection werden die Zeitstempel für *Zuletzt gesehen* gelöscht. Um einen AP zu bearbeiten, klicken Sie auf die Schaltfläche *Bearbeiten* (siehe *Einen Access Point bearbeiten* unten).

Ausstehende Access Points

Hier werden alle APs aufgeführt, die mit dem System verbunden, aber noch nicht autorisiert sind.Um einen Access Point zu autorisieren, klicken Sie auf die Schaltfläche *Akzeptieren* (siehe *Einen Access Point bearbeiten* unten).

Nachdem ein Access Point seine Konfiguration erhalten hat, ist er autorisiert und wird sofort in einem der oberen Bereiche angezeigt, je nachdem, ob er im Moment aktiv ist oder nicht.

Einen Access Point bearbeiten

1. **Klicken Sie auf die Schaltfläche *Bearbeiten* bzw. *Annehmen* des entsprechenden Access Points.**
   Das Dialogfenster *Access Point bearbeiten* öffnet sich.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Bezeichnung (optional): Geben Sie eine Bezeichnung ein, damit der AP leicht im Netz identifiziert werden kann.

   Land: Geben Sie das Land an, in dem sich der AP befindet.

   > **Wichtiger Hinweis –** Der Ländercode reguliert, welche Kanäle für die Übermittlung zur Verfügung stehen. Um nicht gegen nationale Gesetze zu verstoßen, sollten Sie immer das richtige Land auswählen (siehe Kapitel *Access Points*).

   Gruppe (optional): Sie können APs in Gruppen organisieren. Falls bereits eine Gruppe angelegt wurde, können Sie diese in der Auswahlliste auswählen. Andernfalls wählen Sie << *Neue Gruppe* >> und geben in das angezeigte Textfeld *Name* einen Namen für die Gruppe ein. Gruppen können Sie auf der Registerkarte *Gruppieren* verwalten.

3. **Nehmen Sie im Bereich *WLAN-Netzwerke* die folgenden Einstellungen vor:**
   WLAN-Netzwerk-Auswahl (nur wenn keine Gruppe oder eine neue Gruppe ausgewählt ist): Wählen Sie die WLAN-Netzwerke, die der Access Point ausstrahlen soll, aus. Dies ist beispielsweise nützlich, wenn Sie ein nur in firmeneigenen Büros verfügbares kabelloses Firmennetzwerk sowie ein kabelloses Netzwerk für Gäste haben,

das nur in den öffentlichen Bereichen des Gebäudes verfügbar sein soll. Sie können die Liste der WLAN-Netzwerke mit Hilfe des Filterfelds in der Listenüberschrift durchsuchen.

> **Hinweis –** Damit ein Access Point ein WLAN-Netzwerk ausstrahlen kann, müssen einige Bedingungen erfüllt sein. Diese werden im Abschnitt Regeln für das Zuweisen von Netzwerken zu APs erläutert.

4. **Nehmen Sie optional im Bereich *Mesh-Netzwerke* die folgenden Einstellungen vor** (nur verfügbar mit AP 50 und nur, wenn auf der Registerkarte *Mesh-Netzwerke* ein Mesh-Netzwerk definiert ist):
   Mesh-Rollen: Klicken Sie auf das Plussymbol, um Mesh-Netzwerke auszuwählen, die von dem Access Point ausgestrahlt werden sollen. Ein Dialogfenster öffnet sich.

   - **Mesh:** Wählen Sie das Mesh-Netzwerk.
   - **Rolle:** Definieren Sie die Rolle des Access Points für das gewählte Mesh-Netzwerk. Ein Root-Access-Point ist direkt mit der UTM verbunden. Ein Mesh-Access-Point wird sich, nachdem er seine initiale Konfiguration erhalten hat und von der UTM getrennt ist, über das Mesh-Netzwerk mit einem Root-Access-Point verbinden. Beachten Sie, dass ein Access Point nur für ein einziges Mesh-Netzwerk Mesh-Access-Point sein kann.

   Nach dem Speichern wird die Rolle des Access Points durch das Access-Point-Symbol in der Liste *Mesh-Rollen* angezeigt. Über die Funktions-Symbole können Sie eine Mesh-Rolle bearbeiten oder aus der Liste löschen.

   > **Wichtiger Hinweis –** Wenn Sie eine Mesh-Rolle aus der Liste *Mesh-Rollen* löschen, müssen Sie den Access Point wieder mit Ihrem Ethernet verbinden, damit er seine initiale Konfiguration erhält. Um das Mesh-Netzwerk zu ändern ohne den Access Point wieder mit dem Ethernet verbinden zu müssen, löschen Sie die Mesh-Rolle nicht, sondern klicken Sie stattdessen auf das Bearbeiten-Symbol der Mesh-Rolle und wählen Sie das gewünschte Mesh-Netzwerk.

5. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   2,4-GHz-Kanal: Sie können die Standardeinstellung *Auto* beibehalten, mit der automatisch der am wenigsten verwendete Kanal zur Übertragung verwendet wird. Alternativ können Sie einen festen Kanal auswählen.

5-GHz-Kanal (Nur verfügbar mit AP 50): Sie können die Standardeinstellung *Auto* beibehalten, mit der automatisch der am wenigsten verwendete Kanal zur Übertragung verwendet wird. Alternativ können Sie einen festen Kanal auswählen.

Tipp – Wenn Sie *Auto* auswählen, wird der aktuell verwendete Kanal beim Eintritt in den Access Point bekannt gegeben.

TX Power 2,4 GHz: Sie können die Standardeinstellung von *100 %* beibehalten, damit der Access Point mit maximaler Leistung sendet. Sie können die Sendeleistung auch nach unten regeln, um die Reichweite zu verringern und damit zum Beispiel Störungen zu vermeiden.

TX Power 5 GHz (Nur verfügbar mit AP 50): Beim AP 50 können Sie die Sendeleistung für das 5-GHz-Frequenzband separat regeln.

STP: Um das Spanning Tree Protocol zu aktivieren, wählen Sie *Aktiviert* aus der Auswahlliste aus. Dieses Netzwerkprotokoll erkennt und verhindert Bridge-Loops. STP ist obligatorisch, wenn der Access Point ein Mesh-Netzwerk überträgt.

VLAN-Taggen: VLAN-Taggen ist standardmäßig ausgeschaltet. Wenn Sie den AP mit einer vorhandenen VLAN-Ethernet-Schnittstelle verbinden möchten, müssen Sie das Auswahlkästchen auswählen, um VLAN-Taggen zu aktivieren.Stellen Sie sicher, dass die VLAN-Ethernet-Schnittstelle im Feld *Zugelassene Schnittstellen* auf der Seite *Allgemeine Einstellungen* > *Allgemeine Einstellungen* hinzugefügt ist.

Hinweis – Gehen Sie wie folgt vor, um VLAN mit den Access Points in Ihrem Netzwerk zu nutzen: Verbinden Sie den AP für mindestens eine Minute über das Standard-LAN mit der UTM. Das ist notwendig, damit sich der AP seine Konfiguration abholen kann. Würde der AP gleich über VLAN verbunden, wüsste er nicht, dass er sich in einem VLAN befindet, und könnte sich deshalb nicht mit der UTM verbinden, um seine Konfiguration zu erhalten. Wenn der AP angezeigt wird, aktivieren Sie VLAN-Taggen und geben Sie die VLAN-ID ein. Verbinden Sie den AP dann mit dem vorgesehenen VLAN, zum Beispiel einem Switch.

Hinweis – VLAN-Taggen ist mit dem AP 5 nicht möglich.

AP VLAN-ID: Wenn *VLAN-Tagging* aktiviert ist, geben Sie das VLAN-Tag des VLAN ein, über das der Access Point eine Verbindung mit der UTM herstellen soll.Verwenden Sie nicht die VLAN-Tags `0` und `1`, da diese gewöhnlich eine spezielle Bedeutung für Netzwerk-Hardware wie Switches haben. `4095` ist zudem per Konvention reserviert.

Hinweis – Wenn VLAN-Taggen konfiguriert ist, wird der AP auf dem konfigurierten VLAN 60 Sekunden lang nach DHCP suchen. Wenn er in diesem Zeitraum keine IP-Adresse erhält, wird der AP ersatzweise auf dem regulären LAN nach DHCP suchen.

6. **Klicken Sie auf *Speichern*.**
   Der Access Point erhält seine Konfiguration oder seine Konfiguration wird aktualisiert.

Hinweis – Eine Konfigurationsänderung dauert etwa 15 Sekunden. Danach sind alle Schnittstellen neu konfiguriert.

Falls VLAN-Taggen konfiguriert wurde, der AP sich aber nicht mit der UTM über VLAN verbinden kann, wird der AP sich selbst neu starten und es erneut versuchen, nachdem er die Konfiguration erhalten hat.

Regeln für das Zuweisen von Netzwerken zu APs

Damit ein Access Point einem WLAN-Netzwerk zugewiesen werden kann, müssen die Option *Client-Verkehr* des WLAN-Netzwerks und die Option *VLAN-Taggen* des Access Points zueinanderpassen. Folgende Regeln gelten:

- WLAN-Netzwerk mit Client-Verkehr *Getrennte Zone*: VLAN-Taggen für den Access Point kann eingeschaltet oder ausgeschaltet sein.
- WLAN-Netzwerk mit Client-Verkehr *In AP-LAN bridgen*: VLAN-Taggen für den Access Point muss ausgeschaltet sein.
- WLAN-Netzwerk mit Client-Verkehr *In VLAN bridgen*: VLAN-Taggen für den Access Point muss eingeschaltet sein.Die jeweiligen WLAN-Clients verwenden die für das WLAN-Netzwerk festgelegte VLAN-ID (*In VLAN-ID bridgen*) oder erhalten ihre VLAN-ID vom RADIUS-Server, sofern angegeben.

Hinweis – Einem AP 5 kann nur ein einziges WLAN-Netzwerk mit der *Client-Verkehr*-Option *In AP-LAN bridgen* zugewiesen werden.

12.3.2 Gruppierung

Auf der Seite *Wireless Protection > Access Points > Gruppierung* können Sie Access Points in Gruppen organisieren. Die Liste bietet einen Überblick über alle Access-Point-Gruppen und alle Access Points, die keiner Gruppe zugehören. Access Points und Gruppen können durch ihr jeweiliges Symbol unterschieden werden.

Um eine Access-Point-Gruppe anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Gruppierung* auf *Neue Gruppe*.**
   Das Dialogfeld *Neue Access-Point-Gruppe* öffnet sich.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Access-Point-Gruppe ein.

   VLAN-Taggen: VLAN-Taggen ist standardmäßig ausgeschaltet. Wenn Sie den AP mit einer vorhandenen VLAN-Ethernet-Schnittstelle verbinden möchten, müssen Sie das Auswahlkästchen auswählen, um VLAN-Taggen zu aktivieren. Stellen Sie sicher, dass die VLAN-Ethernet-Schnittstelle im Feld *Zugelassene Schnittstellen* auf der Seite *Allgemeine Einstellungen > Allgemeine Einstellungen* hinzugefügt ist.

   - **AP VLAN-ID:** Geben Sie das VLAN-Tag ein, der von dieser AP-Gruppe zur Verbindung mit der UTM verwendet werden soll. Verwenden Sie nicht die VLAN-Tags `0` und `1`, da diese gewöhnlich eine spezielle Bedeutung für Netzwerk-Hardware wie Switches haben. `4095` ist zudem per Konvention reserviert.

   Auswahl von Access Points: Wählen Sie die Access Points aus, die Sie zur Gruppe hinzufügen möchten. Es werden nur Access Points angezeigt, die keiner Gruppe angehören.

   Auswahl von WLAN-Netzwerken: Wählen Sie die WLAN-Netzwerke, die von den Access Points dieser Gruppe ausgestrahlt werden sollen.

   > **Hinweis –** Damit ein Access Point ein WLAN-Netzwerk ausstrahlen kann, müssen einige Bedingungen erfüllt sein. Sie sind im Kapitel *Access Points > Übersicht*, Abschnitt Regeln für das Zuweisen von Netzwerken zu APs, beschrieben.

3. **Klicken Sie auf *Speichern*.**
   Die neue Access-Point-Gruppe wird in der Liste *Gruppierung* angezeigt.

Um eine Access-Point-Gruppe zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen einer Gruppe.

Um einen Access Point zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen eines Access Points. Mehr Informationen zum Bearbeiten und Löschen von Access Points finden Sie im Kapitel *Access Points* > *Übersicht*.

12.4 Mesh-Netzwerke

Auf der Seite *Wireless Protection* > *Mesh-Netzwerke* können Sie vermaschte Netzwerke (engl. Mesh Networks) definieren und ihnen die Access Points zuordnen, die sie übertragen. In einem Mesh-Netzwerk kommunizieren generell mehrere Access Points miteinander, die das gleiche WLAN-Netzwerk ausstrahlen. Zum einen können Access Points, die durch ein Mesh-Netzwerk verbunden sind, das gleiche WLAN-Netzwerk an Clients übertragen und so wie ein einzelner Access Point arbeiten, und dabei ein größeres Gebiet abdecken. Zum anderen kann ein Mesh-Netzwerk dazu verwendet werden, Ethernet-Netzwerke kabellos zu bridgen.

In Mesh-Netzwerken verwendete Access Points können eine von zwei Rollen spielen: Root-Access-Point oder Mesh-Access-Point. Beide übertragen das Mesh-Netzwerk, wodurch sich die Anzahl anderer WLAN-Netzwerke, die sie übertragen können, um eins reduziert.

- **Root-Access-Point:** Dieser besitzt eine Kabelverbindung zur UTM und stellt ein Mesh-Netzwerk zur Verfügung. Ein Access Point kann für mehrere Mesh-Netzwerke Root-Access-Point sein.
- **Mesh-Access-Point:** Dieser benötigt ein Mesh-Netzwerk, um sich über einen Root-Access-Point mit der UTM zu verbinden. Ein Access Point kann nur für ein einziges Mesh-Netzwerk Mesh-Access-Point sein.

Für Mesh-Netzwerke gibt es zwei wesentliche Einsatzzwecke: WLAN-Bridge und WLAN-Repeater.

- **WLAN-Bridge:** Mithilfe von zwei Access Points können Sie eine kabellose Verbindung zwischen zwei Ethernet-Segmenten einrichten. Eine WLAN-Bridge ist hilfreich, wenn es nicht möglich ist, diese Netzwerksegmente durch ein Kabel zu verbinden. Das erste Ethernet-Segment, in dem sich die UTM befindet, ist mit der Ethernet-Schnittstelle des Root-Access-Points verbunden, während das zweite Ethernet-Segment mit der Ethernet-Schnittstelle des Mesh-Access-Points verbunden sein muss. Mit Hilfe mehrerer Mesh-Access-Points können Sie auch mehrere Ethernet-Segmente miteinander verbinden.



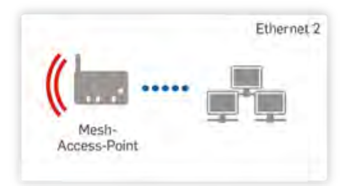
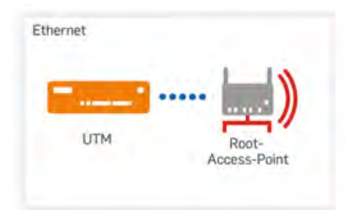


Bild 22 Mesh-Netzwerk, eingesetzt als WLAN-Bridge

- **WLAN-Repeater:** Ihr Ethernet mit der UTM ist mit der Ethernet-Schnittstelle des Root-Access-Points verbunden. Der Root-Access-Points besitzt über das Mesh-Netzwerk eine WLAN-Verbindung mit dem Mesh-Access-Point, der WLAN-Netzwerke an WLAN-Clients überträgt.



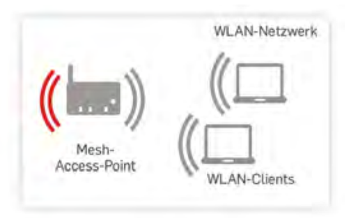


Bild 23 Mesh-Netzwerk, eingesetzt als WLAN-Repeater

Um ein Mesh-Netzwerk anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Seite *Mesh-Netzwerke* auf *Mesh-Netzwerk hinzufügen*.**
   Das Dialogfeld *Mesh-Netzwerk hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Mesh-ID: Geben Sie einen eindeutigen Bezeichner für das Mesh-Netzwerk ein.

   Frequenzband: Access Points, die diesem Netzwerk zugeordnet sind, übertragen das Mesh-Netzwerk auf dem gewählten Frequenzband. Generell ist es sinnvoll, für das Mesh-Netzwerk ein anderes Frequenzband zu wählen als für die ausgestrahlten WLAN-Netzwerke.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

   Access Points: Klicken Sie auf das Plussymbol und wählen Sie die Access Points aus, die das Mesh-Netzwerk ausstrahlen sollen. Das Dialogfenster *Mesh-Rolle hinzufügen* öffnet sich:

- **AP:** Wählen Sie einen Access Point. Beachten Sie, dass zurzeit nur AP-50-Access-Points Mesh-Netzwerke übertragen können.
- **Rolle:** Definieren Sie die Rolle des Access Points für das gewählte Mesh-Netzwerk. Ein Root-Access-Point ist direkt mit der UTM verbunden. Ein Mesh-Access-Point wird sich, nachdem er seine initiale Konfiguration erhalten hat und von der UTM getrennt ist, über das Mesh-Netzwerk mit einem Root-Access-Point verbinden. Beachten Sie, dass ein Access Point nur für ein einziges Mesh-Netzwerk Mesh-Access-Point sein kann.

Hinweis – Für die initiale Konfiguration des Mesh-Access-Points ist es entscheidend, dass er, wie jeder andere Access Point auch, mit einem der Ethernet-Segmente verbunden ist, die auf der Registerkarte *Allgemeine Einstellungen* im Feld *Zugelassene Schnittstellen* ausgewählt sind.

Verwenden Sie das Löschen-Symbol in der Liste *Access Points*, um einen Access Point von der Liste zu löschen.

Wichtiger Hinweis – Wenn Sie einen Mesh-Access-Point von der Liste *Access Points* löschen, müssen Sie ihn wieder mit Ihrem Ethernet verbinden, damit er seine initiale Konfiguration erhält. Um ein anderes Mesh-Netzwerk auszuwählen, ohne den Access Point wieder mit dem Ethernet verbinden zu müssen, löschen Sie den Access Point nicht, sondern gehen Sie folgendermaßen vor: Klicken Sie auf der Registerkarte *Access Points* > *Übersicht* auf die Schaltfläche *Bearbeiten* des Access Points, klicken Sie im Bereich *Mesh-Netzwerke* auf das Bearbeiten-Symbol und wählen Sie das gewünschte Mesh-Netzwerk aus.

Das Symbol eines Access Points zeigt die Rolle des Access Points an. Mit Hilfe des Filterfeldes in der Listenüberschrift können Sie in der Access-Point-Liste suchen.

3. **Klicken Sie auf *Speichern*.**
   Ihre Einstellungen werden gespeichert. Das Mesh-Netzwerk wird in der Liste *Mesh-Netzwerke* angezeigt.

12.5 WLAN-Clients

Die Seite *Wireless Protection > WLAN-Clients* gibt Ihnen einen Überblick über die Clients, die momentan mit einem Access Point verbunden sind oder in der Vergangenheit verbunden waren.

Da nicht alle Clients ihren Namen übermitteln, können Sie ihnen hier einen Namen geben, damit Sie bekannte Clients in der Übersicht leichter auseinanderhalten können. Falls Clients ihren NetBIOS-Namen während der DHCP-Anfrage übermitteln, wird ihr Name in der Tabelle angezeigt. Andernfalls werden sie als *[unknown]* aufgeführt. Sie können den Namen von (unbekannten) Clients ändern, indem Sie auf das Schlüsselsymbol vor dem Namen klicken. Geben Sie dann einen Namen ein und klicken Sie auf *Speichern*. Es dauert ein paar Sekunden, bis die Änderung sichtbar wird. Klicken Sie auf das Aktualisieren-Symbol in der rechten oberen Ecke des WebAdmin, um den Namen des Clients zu sehen.

Sie können Clients auch aus der Tabelle löschen, indem Sie auf das Leeren-Symbol in der ersten Spalte klicken.

Bei einem Neustart des Dienstes Wireless Protection werden die Zeitstempel für *Zuletzt gesehen* gelöscht.

Hinweis – IP-Adressen, die Clients zugewiesen sind, können nur angezeigt werden, wenn UTM als DHCP-Server für das entsprechende WLAN-Netzwerk fungiert. Außerdem wird für statische DHCP-Zuweisungen momentan die IP-Adresse `0.0.0.0` angezeigt.

12.6 Hotspots

Auf den Seiten *Wireless Protection > Hotspots* verwalten Sie den Zugang zum Hotspotportal. Die Hotspot-Funktion ermöglicht es, in Gaststätten, Hotels, Unternehmen usw. Gästen einen zeit- und volumenbeschränkten Internetzugang bereitzustellen. Die Funktion ist Teil des Wireless-Abonnements, funktioniert aber auch in LAN-Netzwerken.

Hinweis – Technisch gesehen beschränkt die Hotspot-Funktion Datenverkehr, der von der Firewall freigegeben ist. Sie müssen daher eine Firewallregel erstellen, die den Datenverkehr

über die Hotspots regelt. Testen Sie den Zugang erst einmal ohne die Hotspot-Funktion. Wenn alles funktioniert, aktivieren Sie die Hotspots.

Hinweis – Wenn die Hotspot-Funktion in Kombination mit einem aktiv-aktiv-Cluster-Aufbau verwendet wird, lässt sich der betreffende Verkehr nicht auf Master und Workers aufteilen. Der gesamte Verkehr von und zu den Hotspot-Schnittstellen wird über den Master geleitet.

Erstellen von Hotspots

In einem ersten Schritt erstellt und aktiviert der Administrator einen Hotspot für einen bestimmten Zugangstyp. Die folgenden Typen sind verfügbar:

- **Annahme der Nutzungsbedingungen:** Dem Gast werden Nutzungsbedingungen angezeigt, die er akzeptieren muss, um Zugang zu erhalten. Die Bedingungen sind frei definierbar.
- **Tages-Kennwort:** Der Gast muss ein Zugangskennwort eingeben. Das Kennwort wird täglich geändert.
- **Voucher:** Der Gast erhält einen Voucher mit einem Zugangscode, den er eingeben muss. Der Voucher kann auf eine bestimmte Anzahl Geräte, einen Zeitraum oder ein Datenvolumen beschränkt sein.

Verteilung der Zugangsdaten an Gäste

Bei den Typen *Tages-Kennwort* und *Voucher* müssen die Zugangsdaten den Gästen ausgehändigt werden. Sie können festlegen, welche Benutzer die Zugangsdaten verwalten und verteilen dürfen. Diese Benutzer greifen über die Benutzerportal-Registerkarte *Hotspot* auf die Daten zu und können sie von dort aus auch verteilen:

- **Tages-Kennwort:** Benutzer finden das Kennwort im Benutzerportal. Das Kennwort kann per E-Mail versendet werden. Benutzer leiten das Kennwort an die Gäste weiter. Sie können ein neues Kennwort eingeben oder generieren. In diesem Fall wird das vorhergehende Kennwort sofort ungültig. Alle laufenden Sitzungen werden beendet. Je nach Konfiguration werden auch andere Benutzer über das neue Kennwort in Kenntnis gesetzt, entweder per E-Mail oder über das Benutzerportal.
- **Voucher:** Im Benutzerportal können Benutzer Voucher mit einmaligen Zugangscodes erstellen. Der Administrator kann verschiedene Voucher-Typen definieren und

bereitstellen. Sie können Voucher ausdrucken, exportieren und den Gästen aushändigen. Die Liste der erstellten Voucher liefert einen Überblick über ihre Nutzung und erleichtert ihre Verwaltung.

Rechtliche Hinweise

In vielen Ländern unterliegt der Betrieb eines öffentlichen WLAN gesetzlichen Regelungen, dazu gehören unter anderem Zugriffsbeschränkungen auf Websites mit bestimmten Inhalten (z. B. File-Sharing-Seiten, Seiten mit extremistischem Hintergrund usw.). Sie können diese Anforderungen erfüllen, indem Sie den Hotspot mit den Web-Protection-Funktionen von Sophos UTM kombinieren, um den Webzugriff auf ganze Websites oder bis hinunter auf die Ebene einzelner URLs zu blockieren oder zuzulassen. Mit UTM haben Sie volle Kontrolle darüber, wer wann auf welche Seiten zugreifen kann. So ist es auch möglich, für den Hotspot besonders strikte Regeln festzulegen, wenn staatliche oder unternehmensinterne Auflagen dies erfordern.

Der integrierte HTTP-Proxy von Sophos UTM bietet zusätzlich leistungsfähige Protokoll- und Berichtsfunktionen. Sie können zum Beispiel verfolgen, welche Personen wann und wie oft auf welche Websites zugreifen und so leicht eine unangemessene Nutzung identifizieren, wenn Sie einen Hotspot ohne jegliche Zugangsbeschränkungen betreiben.

In bestimmten Fällen kann es möglich sein, dass Sie Ihren Hotspot bei der staatlichen Regulierungsbehörde anmelden müssen.

12.6.1 Allgemein

Auf der Registerkarte *Wireless Protection* > *Hotspots* > *Allgemein* können Sie die Hotspots-Funktion einschalten und angeben, welche Benutzer die Hotspot-Zugangsdaten anzeigen und verteilen können.

Um Hotspots zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Hotspots auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und der Abschnitt *Allgemeine Hotspot-Einstellungen* kann nun bearbeitet werden.

2. **Wählen Sie die zugelassenen Benutzer aus.**
   Wählen Sie die Benutzer oder Gruppen aus, die Zugriff auf das Benutzerportal haben sollen, oder fügen Sie neue Benutzer hinzu. Die hier ausgewählten Benutzer können das

Tages-Kennwort anzeigen und Hotspot-Voucher erstellen. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Live-Protokoll

Das Live-Protokoll liefert Informationen über die Hotspot-Nutzung. Klicken Sie auf *Live-Protokoll öffnen*, um das Hotspots-Live-Protokoll in einem neuen Fenster zu öffnen.

Vorlagen herunterladen

Hier können Sie die Hotspot-Anmeldungsvorlage und die Voucher-Vorlage herunterladen, die beim Hinzufügen eines neuen Hotspots standardmäßig verwendet werden. Sie können die Standardvorlagen bearbeiten, um Ihre Hotspot-Anmeldeseite oder das Voucher-Design anzupassen, ohne sie von Grund auf neu erstellen zu müssen. Sie können die angepasste HTML- und PDF-Vorlage auf der Registerkarte *Wireless Protection > Hotspots > Hotspots* hochladen.

1. **Klicken Sie auf das blaue Download-Symbol.**
   Das Dialogfenster *Zertifikatdatei herunterladen* wird geöffnet.

2. **Speichern Sie die Datei.**
   Die Datei wird heruntergeladen.

12.6.2 Hotspots

Auf der Registerkarte *Wireless Protection > Hotspots > Hotspots* verwalten Sie Ihre Hotspots.

Hinweis – Ein Hotspot muss einer existierenden Schnittstelle zugewiesen sein; in der Regel wird das eine WLAN-Schnittstelle sein. Alle Hosts, die diese Schnittstelle verwenden, unterliegen automatisch den Beschränkungen dieses Hotspots. Bevor Sie einen Hotspot erstellen, legen Sie daher üblicherweise zuerst ein WLAN-Netzwerk mit der Option *Getrennte Zone* und danach eine Schnittstelle für die entsprechende WLAN-Schnittstellenhardware an. Weitere Informationen hierzu finden Sie unter *Wireless Protection > WLAN-*Netzwerke.

Um einen Hotspot anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Hotspot hinzufügen*.**
   Das Dialogfeld *Hotspot hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diesen Hotspot ein.

   Schnittstellen: Fügen Sie die Schnittstellen hinzu, für die die Zugriffsbeschränkungen des Hotspots gelten sollen. Für die ausgewählten Schnittstellen muss eine Firewallregel existieren, die den gewünschten Datenverkehr zulässt. Eine Schnittstelle kann immer nur von einem Hotspot verwendet werden.

   Warnung – Sie sollten hier keine Uplink-Schnittstelle auswählen, da anschließend Verkehr ins Internet komplett blockiert ist. Außerdem raten wir dringend davon ab, Schnittstellen zu verwenden, die von Servern benutzt werden, die essenzielle Dienste wie Authentifizierung zur Verfügung stellen. Sie können sich dadurch unwiderruflich vom WebAdmin ausschließen!

   Hotspot-Typ: Wählen Sie den Hotspot-Typ für die ausgewählten Schnittstellen.

   - **Tages-Kennwort:** Einmal am Tag wird automatisch ein neues Kennwort erstellt. Dieses Kennwort kann im Benutzerportal auf der Registerkarte *Hotspots* von allen auf der Registerkarte *Allgemein* festgelegten Benutzern eingesehen werden. Außerdem wird das Kennwort an die angegebenen E-Mail-Adressen gesendet.
   - **Voucher** (nicht verfügbar mit BasicGuard-Abonnement): Wählen Sie diesen Hotspot-Typ, um im Benutzerportal zeit- oder volumenbeschränkte Gutscheine mit benutzerdefinierten Eigenschaften zu erstellen, die sich ausdrucken und an Kunden verteilen lassen. Nach Eingabe des Codes erhalten die Kunden Zugang zum Internet.
   - **Annahme der Nutzungsbedingungen:** Kunden erhalten erst nach Annahme der Nutzungsbedingungen Zugang zum Internet.
   - **Backend-Authentifizierung:** Bei diesem Hotspot-Typ können sich Benutzer über einen beliebigen unterstützten Backend-Mechanismus authentifizieren (siehe *Definitionen & Benutzer > Authentifizierungsdienste*). Bei diesem Typ werden die Benutzerzugangsdaten gespeichert, um periodisch zu überprüfen, ob der Benutzer noch autorisiert ist.

   Hinweis – Wenn Sie *Backend-Authentifizierung* auswählen, wird im Anmeldeformular ein neues Eingabefeld für OTP-Token angezeigt (falls Hotspot als OTP-Einrichtung konfiguriert ist).

Kennwort erstellt um (nur bei Hotspot-Typ *Tages-Kennwort*): Die Tageszeit, zu der das neue Kennwort erstellt wird. Zu dieser Uhrzeit wird das bisherige Kennwort ungültig. Alle laufenden Sitzungen werden beendet.

Kennwort per E-Mail senden an (nur bei Hotspot-Typ *Tages-Kennwort*): Fügen Sie E-Mail-Adressen hinzu, an die das Kennwort gesendet werden soll.

Voucher-Definitionen (nur bei Hotspot-Typ *Voucher*): Fügen Sie die Voucher-Definitionen für Ihren Hotspot hinzu oder wählen Sie sie aus. Das Hinzufügen einer Voucher-Definition wird auf der Seite *Voucher-Definitionen* erläutert.

Geräte pro Voucher (nur bei Hotspot-Typ *Voucher*): Geben Sie an, wie viele Geräte sich maximal mit einem Voucher während seines Gültigkeitszeitraums einloggen können. Die Option *unbegrenzt* wird nicht empfohlen.

Hotspot-Benutzer (nur bei Hotspot-Typ *Backend-Authentifizierung*): Wählen Sie die Benutzer oder Benutzergruppen aus, die über Backend-Authentifizierung Zugriff auf den Hotspot haben sollen, oder fügen Sie die Benutzer hinzu. Normalerweise handelt es sich dabei um eine Backend-Benutzergruppe.

Ablauf der Sitzung (nur bei Hotspot-Typ *Annahme der Nutzungsbedingungen* oder *Backend-Authentifizierung*): Geben Sie hier einen Zeitraum für die Gültigkeit des Internetzugangs an.Nach Ablauf dieses Zeitraums müssen Benutzer beim Hotspot-Typ *Annahme der Nutzungsbedingungen* die Nutzungsbedingungen erneut akzeptieren, um sich wieder einloggen zu können. Beim Hotspot-Typ *Backend-Authentifizierung* müssen sich die Benutzer wieder authentifizieren.

Benutzer müssen die Nutzungsbedingungen annehmen (außer beim Hotspot-Typ *Annahme der Nutzungsbedingungen*): Wählen Sie diese Option, wenn die Hotspot-Nutzer Ihre Nutzungsbedingungen akzeptieren müssen, um Zugang zum Internet zu erhalten.

- **Nutzungsbedingungen:** Geben Sie hier den Text für die Nutzungsbedingungen ein. Einfache HTML-Befehle und Hyperlinks sind gestattet.

Nach dem Login zu URL weiterleiten: Wählen Sie diese Option, wenn die Nutzer nach Eingabe des Kennworts oder der Voucher-Daten automatisch zu einer bestimmten URL, beispielsweise Ihrer Hotel-Website oder einer Webseite mit Ihren Portal-Richtlinien, weitergeleitet werden sollen.

- **URL:** URL, zu der die Nutzer weitergeleitet werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden Hotspot-Einstellungen vornehmen:** Standardmäßig wird dem Benutzer eine Anmeldeseite mit dem Sophos-Logo angezeigt. Sie können eine angepasste HTML-Datei mit eigenen Bildern und Stylesheets verwenden. Außerdem können Sie das Voucher-Layout anpassen.

   Anpassungstyp: Wählen Sie den Anpassungstyp aus. Die folgenden Typen sind verfügbar:

   - **Grundlegend:** Verwenden Sie die Standard-Anmeldeseitenvorlage.Passen Sie bei Bedarf Logo, Titel und Text an.
     Logo: Laden Sie ein Logo für die Anmeldeseite hoch. Es werden Bilddateien der Formate jpg, png und gif unterstützt. Das Bild sollte nicht breiter als 300 Pixel und höher als 100 Pixel sein (abhängig von der Länge des Titels). Verwenden Sie die Schaltfläche *Standard wiederherstellen*, um wieder das Standardlogo von Sophos auszuwählen.

     Logo auf empfohlene Größe skalieren: Wenn diese Option ausgewählt wird, werden Logos, deren Breite oder Höhe die empfohlenen Werte überschreitet, skaliert und in der empfohlenen Größe angezeigt. Wird sie nicht ausgewählt, wird das Logo in der ursprünglichen Größe angezeigt.

     Titel: Geben Sie hier einen Titel für die Anmeldeseite ein. Einfache HTML-Befehle und Hyperlinks sind gestattet.

     Benutzerdefinierter Text: Geben Sie hier zusätzlichen Text für die Anmeldeseite ein. Sie können zum Beispiel die SSID des WLAN-Netzwerks eingeben. Einfache HTML-Befehle und Hyperlinks sind gestattet.

   - **Komplett:** Wählen Sie eine individuelle HTML-Anmeldeseite aus.
     Anmeldeseitenvorlage: Wählen Sie die HTML-Vorlage aus, die Sie für Ihre individuelle Anmeldeseite verwenden möchten. Klicken Sie auf das Ordnersymbol, um ein Fenster zu öffnen, in dem Sie die Datei auswählen und hochladen können. Verwenden Sie die Schaltfläche *Standard wiederherstellen*, um wieder die Standard-HTML-Vorlage von Sophos auszuwählen. In dieser Vorlage können Sie Variablen verwenden, mit denen sich dynamisch Informationen für jeden Hotspot einfügen lassen. Beispielsweise können Sie den Firmennamen und Administratorinformationen, die Nutzungsbedingungen und das Anmeldeformular

hinzufügen. Detaillierte Informationen finden Sie unter *Verwendung von Variablen in der Anmeldeseitenvorlage*. Sie können die Standard-HTML-Vorlage auf der Registerkarte *Wireless Protection > Hotspots > Allgemein* herunterladen.

Bilder/Stylesheets: Fügen Sie Dateien hinzu, auf die in Ihrer Anmeldeseitenvorlage verwiesen wird, z. B. Bilder, Stylesheets oder JavaScript-Dateien. Klicken Sie auf das Ordnersymbol, um ein Fenster zu öffnen, in dem Sie die Dateien auswählen und hochladen können.

Voucher-Vorlage (nur bei Hotspot-Typ *Voucher*): Klicken Sie auf das Ordnersymbol, um ein Fenster zu öffnen, in dem Sie die PDF-Datei mit dem Voucher-Layout auswählen und hochladen können. Standardmäßig wird eine Standardvorlage verwendet. Klicken Sie auf die Schaltfläche *Standard wiederherstellen*, um den Standard wiederherzustellen. Die Voucher-PDF-Datei muss der PDF-Version PDF 1.5 oder niedriger entsprechen. Ihr Seitenformat und ihre Formatierung können beliebig sein – beide werden während der Voucher-Erstellung im Benutzerportal angepasst, abhängig vom Seitenformat und der Zahl der Voucher pro Seite, die dort festgelegt sind. Sie können die Standard-PDF-Vorlage auf der Registerkarte *Wireless Protection > Hotspots > Allgemein* herunterladen.

Die PDF-Datei kann die folgenden Variablen enthalten, die während der Voucher-Erstellung im Benutzerportal mit den entsprechenden Werten ersetzt werden:

- Name des WLAN-Netzwerks (SSID): <?ssid0?> (sowie <?ssid1?>, <?ssid2?> usw., wenn das WLAN mehr als einen SSID aufweist)
- Kennwort des WLAN-Netzwerks: <?psk0?> (sowie <?psk1?>, <?psk2?> usw., wenn das WLAN mehr als einen SSID aufweist)
- Voucher-Code: <?code?>
- Voucher-Gültigkeitsdauer: <?validity?>
- Voucher-Datenlimit: <?datalimit?>
- Voucher-Zeitlimit: <?timelimit?>
- QR-Code mit codierten Hotspot-Zugangsdaten: <?qrX?>. Die obere linke Ecke des QR-Codes wird auf der unteren linken Ecke der Variable platziert.

Hinweis – Bei Verwendung von Variablen muss die PDF-Datei die gesamten Zeichensätze der verwendeten Schriftarten enthalten. Wenn eine Variable durch ihren

Wert ersetzt wird und eines der Ersatzzeichen nicht zur Verfügung steht, wird der Wert falsch angezeigt. Wir empfehlen Ihnen, den String `<?abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789?>` zu Ihrer PDF-Datei hinzuzufügen. Er wird während der Voucher-Erstellung automatisch entfernt. Außerdem empfiehlt es sich, für die Variablen eine separate Zeile zu verwenden, da das Layout beschädigt werden könnte, wenn der ersetzte Text zu lang ist.

4. **Klicken Sie auf *Speichern*.**
   Der Hotspot wird erstellt und in der Liste *Hotspots* angezeigt.

Tipp – Nachdem Sie den Hotspot gespeichert haben, können Sie eine Vorschau der Anmeldeseite anzeigen. Klicken Sie dazu beim betreffenden Hotspot in der Liste *Hotspots* auf die Schaltfläche *Vorschau der Anmeldeseite*.

Um einen Hotspot zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Verwendung von Variablen in der Anmeldeseitenvorlage

Die HTML-Vorlage für die Anmeldeseite kann verschiedene Variablen enthalten, mit denen sich dynamisch Informationen für die Hotspot-Anmeldeseite einfügen lassen. Wenn UTM eine Vorlage verarbeitet, um eine Anmeldeseite anzuzeigen, ersetzt es Vorlagenvariablen mit den entsprechenden Werten. Folgende Variablen sind gültig:

- Allgemeine Variablen

  `<?company_text?>`: Angepasster Unternehmenstext, wie unter *Verwaltung > Anpassungen > Allgemein definiert*

  `<?company_logo?>`: Unternehmenslogo, wie unter *Verwaltung > Anpassungen > Allgemein* definiertDie Variable wird durch den Pfad der Logodatei ersetzt. Beispiel: `<img src="<?company_logo?>">`

  `<?admin_contact?>`: Name oder Adresse des Administrators, wie unter *Verwaltung > Anpassungen > Web-Meldungen definiert*

`<?admin_message?>`: Administratorinformation, wie unter *Verwaltung> Anpassungen > Web-Meldungen* definiert (Standard: *Ihr Cache-Administrator ist:*)

`<?error?>`: Fehlermeldung, die beim Versuch, sich anzumelden, angezeigt wird.

- Variablen, die für alle Hotspot-Typen verwendet werden
  `<?terms?>`: Nutzungsbedingungen (wie auf der Seite *Hotspots* definiert)

  `<?redirect_host?>`: Umleitungs-URL, die für den Hotspot angegeben ist (wie auf der Seite *Hotspots* definiert)

  `<?location?>`: vom Benutzer aufgerufene URL

  `<?location_host?>`: Hostname der vom Benutzer aufgerufenen URL

  `<?login_form?>`: Für den betreffenden Hotspot-Typ geeignetes Anmeldeformular: *Textfeld Kennwort*, Textfeld *Token*, Textfelder *Benutzername* und *Kennwort* oder *Annahme*-Kontrollkästchen und Schaltfläche *Anmelden*. Informationen zum Erstellen angepasster Anmeldeformulare finden Sie unter *Benutzerspezifisches Anmeldeformular*.

  `<?asset_path?>` (nur für Anpassungsmodus *Komplett* relevant): Hotspot-spezifisches Verzeichnis für die Speicherung von Bildern oder Stylesheets (Beispiel: `<img src="<?asset_path?>/logo.png">`)

- Variablen, die nur für Hotspots des Typs „Voucher“ verwendet werden
  `<?maclimit?>` Zahl der zulässigen Geräte pro Voucher für diesen Hotspot (wie auf der Seite *Hotspots* definiert)

  `<?numdevices?>`: Zahl der für diesen Voucher verwendeten Geräte

  `<?timeend?>`: Ende des Gültigkeitszeitraums (wie auf der Seite *Voucher-Definitionen* definiert)

  `<?time_total?>`: Insgesamt zulässiges Zeitkontingent (wie auf der Seite *Voucher-Definitionen* definiert)

  `<?time_used?>`: Aufgebrauchtes Zeitkontingent (wie auf der Seite *Voucher-Definitionen* definiert)

  `<?traffic_total?>`: Insgesamt zulässiges Datenvolumen (wie auf der Seite *Voucher-Definitionen* definiert)

  `<?traffic_used?>`: Aufgebrauchtes Datenvolumen (wie auf der Seite *Voucher-Definitionen* definiert)

Vorlagen können *if*-Variablen enthalten, die Abschnitte wie die unten gezeigten bilden. Jeder Abschnitt verfügt über eine öffnende und eine schließende Variable. Der Inhalt eines *if*-Abschnitts wird nur unter einer bestimmten Bedingung angezeigt.

If-Abschnitt	Bedeutung
<?if_loggedin?> <?if_loggedin_end?>	Abschnitt wird angezeigt, wenn sich der Benutzer erfolgreich angemeldet hat.
<?if_notloggedin?> <?if_notloggedin_end?>	Abschnitt wird angezeigt, wenn sich der Benutzer noch nicht angemeldet hat, beispielsweise, weil die Nutzungsbedingungen noch angenommen werden müssen oder ein Fehler aufgetreten ist.
<?if_authtype_password?> <?if_authtype_password_end?>	Abschnitt wird angezeigt, wenn der Hotspot-Typ *Tages-Kennwort* ist.
<?if_authtype_disclaimer?> <?if_authtype_disclaimer_end?>	Abschnitt wird angezeigt, wenn der Hotspot-Typ *Annahme der Nutzungsbedingungen* ist.
<?if_authtype_token?> <?if_authtype_token_end?>	Abschnitt wird angezeigt, wenn der Hotspot-Typ *Voucher* ist.
<?if_authtype_backend?> <?if_authtype_backendtoken_end?>	Abschnitt wird angezeigt, wenn der Hotspot-Typ *Backend-Authentifizierung* ist.
<?if_location?> <?if_location_end?>	Abschnitt wird angezeigt, wenn der Benutzer umgeleitet wurde.

If-Abschnitt	Bedeutung
<?if_redirect_url?> <?if_redirect_url_end?>	Abschnitt wird angezeigt, wenn das Kontrollkästchen *Nach dem Login zu URL weiterleiten* aktiviert ist.
<?if_not_redirect_url?> <?if_not_redirect_url_end?>	Abschnitt wird angezeigt, wenn das Kontrollkästchen *Nach dem Login zu URL weiterleiten* deaktiviert ist.
<?if_timelimit?> <?if_timelimit_end?>	Abschnitt wird angezeigt, wenn für einen Voucher ein Gültigkeitszeitraum festgelegt ist.
<?if_trafficlimit?> <?if_trafficlimit_end?>	Abschnitt wird angezeigt, wenn für einen Voucher ein Datenvolumen festgelegt ist.
<?if_timequota?> <?if_timequota_end?>	Abschnitt wird angezeigt, wenn für einen Voucher ein Zeitkontingent festgelegt ist.
<?if_maclimit?> <?if_maclimit_end?>	Abschnitt wird angezeigt, wenn ein Wert für *Geräte pro Voucher* festgelegt ist.
<?if_terms?> <?if_terms_end?>	Abschnitt wird angezeigt, wenn Nutzungsbedingungen definiert und aktiviert sind.
<?if_error?> <?if_error_end?>	Abschnitt wird angezeigt, wenn beim Anmelden ein Fehler aufgetreten ist.

Benutzerspezifisches Anmeldeformular

Wenn Sie ein eigenes Anmeldeformular erstellen möchten, anstatt die vordefinierte Variable `<?login_form?>` zu verwenden, beachten Sie dabei Folgendes:

- Schließen Sie das Formular in folgende Tags ein:
  ```
  <form action="?action=login" method="POST">...</form>
  ```
- Für einen Hotspot zur Annahme der Nutzungsbedingungen fügen Sie ein Kontrollkästchen namens "accept" ein:
  ```
  <input type="checkbox" name="accept">
  ```
- Für Tages-Kennwort- oder Voucher-Hotspots fügen Sie ein Textfeld namens "token" ein:
  ```
  <input type="text" name="token">
  ```
- Für einen Backend-Authentication-Hotspot fügen Sie zwei Textfelder namens "username" und "password" ein:
  ```
  <input type="text" name="username">
  <input type="password" name="password">
  ```
- Fügen Sie eine Funktion zum Senden des Formulars hinzu, z. B. eine Anmelde-Schaltfläche:
  ```
  <input type="submit" name="login" value="Login">
  ```

12.6.3 Voucher-Definitionen

Auf der Registerkarte *Wireless Protection* > *Hotspots* > *Voucher-Definitionen* verwalten Sie die Definitionen für den Hotspot-Typ „Voucher“.

Um eine Voucher-Definition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Voucher-Definition hinzufügen*.**
   Das Dialogfeld *Voucher-Definition hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Voucher-Definition ein.

   Gültigkeitszeitraum: Geben Sie an, wie lange ein Voucher mit dieser Definition gültig sein soll. Gezählt wird ab der ersten Anmeldung. Die Angabe eines Gültigkeitszeitraums wird empfohlen.

   Hinweis – Der maximale Zeitraum für den *Gültigkeitszeitraum* beträgt zwei Jahre.

   Zeitkontingent: Geben Sie hier die erlaubte Online-Zeit ein. Geben Sie die maximale Online-Zeit ein, nach deren Erreichen ein Voucher mit dieser Definition abläuft. Gezählt

wird von der Anmeldung bis zur Abmeldung. Außerdem wird die Zählung nach 5 Minuten Inaktivität angehalten.

Hinweis – Der maximale Zeitraum für den *Gültigkeitszeitraum* beträgt zwei Jahre.

Datenmenge: Hier können Sie das Datenvolumen beschränken. Geben Sie eine maximale Datenmenge an, die mit dieser Voucher-Definition übertragen werden kann.

Hinweis – Das maximale *Datenvolumen* ist 100 GB.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die Voucher-Definition wird erstellt. Sie steht jetzt zur Erstellung eines Hotspots vom Typ „Voucher“ zur Verfügung.

Um eine Voucher-Definition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

12.6.4 Erweitert

Allgemeine Voucher-Optionen

Hier können Sie einen Zeitraum angeben, nach dem nicht mehr gültige Voucher aus der Datenbank gelöscht werden. Im Hotspot-Protokoll bleiben die Informationen über die gelöschten Voucher erhalten.

Eingeschränkter Zugang zum Internet

Hier können Sie einzelne Hosts oder Netzwerke hinzufügen oder auswählen, auf die alle Benutzer ohne Eingabe eines Kennworts oder Voucher-Codes unbeschränkten Zugriff haben. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

13 Webserver Protection

In diesem Kapitel wird beschrieben, wie Sie die Web Application Firewall von Sophos UTM konfigurieren, die Ihre Webserver vor Angriffen und schädigendem Verhalten schützt.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Web Application Firewall
- Umkehrauthentifizierung
- Zertifikatverwaltung

13.1 Web Application Firewall

Mit der Web Application Firewall (WAF), auch bekannt als Reverse Proxy, können Sie dank Sophos UTM Ihre Webserver vor Angriffen und schädigendem Verhalten wie Cross-Site-Scripting (XSS), SQL-Injection, Directory-Traversal und anderen gefährlichen Angriffen schützen. Sie können externe Adressen (virtuelle Server) definieren, die in die „echten“ Server übersetzt werden, anstatt die DNAT-Regel(n) zu verwenden. Dies ermöglicht es auch, die Server mit Hilfe verschiedener Muster und Erkennungsmethoden zu schützen. Einfach ausgedrückt ermöglicht dieser Bereich von UTM die Anwendung von Bedingungen auf Anfragen, die der Webserver erhält und versendet. Darüber hinaus bietet er Lastausgleich zwischen mehreren Zielen.

13.1.1 Virtuelle Webserver

Auf der Registerkarte *Web Application Firewall > Virtuelle Webserver* können Sie virtuelle Webserver anlegen. Als Teil von UTM bilden diese Webserver die Firewall zwischen dem Internet und Ihren Webservern. Darum wird diese Art der Intervention auch Reverse Proxy genannt.UTM nimmt die Anfragen für die Webserver entgegen und schützt die echten Webserver vor diversen Angriffen. Jeder virtuelle Server entspricht einem echten Webserver und legt die Sicherheitsstufe fest, die angewendet werden soll. Sie können auch mehr als einen echten Webserver in einer virtuellen Webserver-Definition verwenden. Auf diese Weise erzielen Sie einen Lastausgleich für Ihre echten Webserver.

Um einen virtuellen Server hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neuer virtueller Webserver*.**
   Das Dialogfeld *Virtuellen Webserver anlegen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den virtuellen Webserver ein.

   Schnittstelle: Wählen Sie aus der Auswahlliste eine Schnittstelle, über die Zugriff auf den Webserver möglich ist.

   Hinweis – Wenn es Schnittstellen mit einer IPv4 und IPv6 Adresse gibt, wird nur die IPv4 Adresse für die Web Application Firewall genommen. Es ist nicht möglich, Link-Local-Adressen als Frontend-Schnittstelle zu verwenden.

   Art: Legen Sie für die Kommunikation zwischen dem Client und dem virtuellen Webserver *Verschlüsselt (HTTPS)* oder *Reiner Text (HTTP)* fest. Wenn Sie Umkehr-authentifizierung verwenden möchten, empfehlen wir dringend, aus Sicherheitsgründen *Verschlüsselt (HTTPS)* auszuwählen.

   Port: Geben Sie eine Portnummer an, über die der virtuelle Webserver von außen erreicht werden kann.Der Standard ist Port 80 bei *Reiner Text (HTTP)* und Port 443 bei *Verschlüsselt (HTTPS)*.

   Von HTTP auf HTTPS umleiten (nur bei *Verschlüsselt (HTTPS)*): Wenn diese Funktion aktiviert ist, werden Benutzer, die die URL ohne `https://` eingeben, automatisch an den virtuellen Webserver weitergeleitet.

   Zertifikat (nur bei *Verschlüsselt (HTTPS)*): Wählen Sie das Zertifikat des Webservers aus der Auswahlliste. Das Zertifikat muss vorher auf dem Webserver angelegt und auf der Registerkarte *Zertifikatverwaltung > Zertifikate* hochgeladen worden sein.

   > **Domäne**: Dieses Feld enthält den Hostnamen, für den das Zertifikat erstellt wurde.
   >
   > **Domänen** (nur bei SAN-Zertifikaten): WAF unterstützt „Subject Alternative Name“-(SAN-)Zertifikate. Alle Hostnamen, die durch ein Zertifikat abgedeckt sind, werden in diesem Feld aufgelistet. Sie können einen oder mehrere Hostnamen auswählen, indem Sie das Auswahlkästchen vor einem Hostnamen markieren.

   Domänen (nur bei *Reiner Text (HTTP)* oder *Verschlüsselt (HTTPS)* mit Platzhalterzertifikat): Geben Sie die Domänen, für die der Webserver verantwortlich ist, als

FQDN ein, z. B. `shop.beispiel.de`, oder verwenden Sie das Aktionssymbol, um eine Liste von Domänennamen zu importieren. Sie können für das Präfix der Domäne einen Asterisk als Platzhalter (*) verwenden. Beispiel: `*.meinedomäne.de`. Domänen mit Platzhaltern werden als Ersatzeinstellungen angesehen: Der virtuelle Webserver mit der Platzhalterdomäne wird nur verwendet, wenn kein anderer virtueller Webserver mit einem spezifischeren Domänennamen konfiguriert ist.Beispiel: Eine Client-Anfrage nach `a.b.c` wird als Erstes `a.b.c` zugeordnet, dann `*.b.c` und dann `*.c`.

Falls *Von HTTP auf HTTPS umleiten* aktiviert ist, muss mindestens eine Domäne ohne Platzhalter als Ziel der Umleitung konfiguriert sein (eine Platzhalterdomäne ist kein gültiges Ziel für die Umleitung). Die erste Domäne, die ohne Platzhalter in der Domänenliste aufgeführt ist, wird als Umleitungsziel verwendet.

Echte Webserver: Erstellen Sie einen neuen echten Webserver oder markieren Sie das Auswahlkästchen vor dem Webserver, dem Sie das Firewall-Profil zuweisen wollen. Wenn Ihre Webserver gespiegelt sind, können Sie auch mehr als einen Webserver auswählen. Auf diese Weise erzielen Sie standardmäßig einen Lastausgleich zwischen den ausgewählten Webservern. Der verwendete Anfrageerfassungsalgorithmus ordnet automatisch jede neue Anfrage demjenigen Webserver zu, der aktuell die kleinste Anzahl an aktiven Anfragen besitzt.Auf der Registerkarte *Site-Path-Routing* können Sie detaillierte Verteilungsregeln festlegen.

Firewall-Profil: Wählen Sie aus der Auswahlliste ein Firewall-Profil aus. Dieses Profil wird angewendet, um die gewählten Webserver zu schützen. Sie können auch *Kein Profil* auswählen, um kein Firewall-Profil zu verwenden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Komprimierungsunterstützung deaktivieren (optional): Standardmäßig ist dieses Kontrollkästchen deaktiviert und der Inhalt wird komprimiert gesendet, wenn der Client komprimierte Daten anfordert und der echte Webserver eines der angefragten Komprimierungsschemas unterstützt. Komprimierung erhöht die Übertragungsrate und reduziert die Seitenladezeit. Wenn Websites jedoch falsch angezeigt werden oder bei Benutzern, die auf Ihre Webserver zugreifen, Inhaltsverschlüsselungsfehler auftreten, kann es erforderlich sein, die Komprimierungsunterstützung zu deaktivieren. Wenn das Kontrollkästchen aktiviert ist, fordert die WAF unkomprimierte Daten von den echten Webser-

vern diese virtuellen Webservers an und sendet sie unkomprimiert an den Client (unabhängig vom Verschlüsselungsparameter der HTTP-Anfrage).

HTML umschreiben (optional): Wählen Sie diese Option, damit UTM die Links der zurückgegebenen Webseiten umschreibt, sodass die Links weiterhin funktionieren.Beispiel: Eine Ihrer echten Webserver-Instanzen hat den Hostnamen ihrefirma.local, aber der Hostname des virtuellen Servers auf UTM lautet ihrefirma.com. Daher funktionieren absolute Links wie <a href="http://ihrefirma.local/"> nicht mehr, wenn der Link vor Weitergabe an den Client nicht in <a href="http://ihrefirma.com/"> umgeschrieben wird. Sie brauchen diese Option jedoch nicht zu aktivieren, wenn ihrefirma.com auf Ihrem Webserver konfiguriert ist oder wenn interne Links auf Ihren Websites immer als relative Links geschrieben sind.Es wird empfohlen, die Option zu verwenden, wenn Sie Microsoft Outlook Web Access und/oder Sharepoint Portal Server einsetzen.

Hinweis – Es ist wahrscheinlich, dass einige Links nicht korrekt umgeschrieben werden können und dadurch nicht funktionieren. Bitten Sie den/die Autor(en) Ihrer Website, Links einheitlich zu formatieren.

Die Funktion HTML-Umschreibung schreibt nicht nur URLs um, sie korrigiert auch fehlerhafte HTML-Syntax, zum Beispiel:

- <title>-Tags werden im DOM-Baum vom Knoten html > title zum richtigen Knoten html > head > title verschoben
- Anführungszeichen um HTML-Attribut-Werte werden korrigiert (z. B. wird aus name="value""name="value")

Hinweis – HTML-Umschreibung wird auf alle Dateien mit HTTP-Inhaltstyp text/* oder *xml* angewandt (* dient als Platzhalter). Stellen Sie sicher, dass andere Dateitypen, z. B. Binärdateien, den richtigen HTTP-Inhaltstyp aufweisen, da sie sonst durch die HTML-Umschreibung beschädigt werden können.

Querverweis – Weitere Informationen finden Sie in der libxml-Dokumentation (http://xmlsoft.org/html/libxml-HTMLparser.html).

Cookie umschreiben (optional, wird nur angezeigt, wenn *HTML umschreiben* aktiviert ist): Wählen Sie diese Option, damit UTM die Cookies der zurückgegebenen Websites umschreibt.

Hinweis – Bei Deaktivierung von *HTML umschreiben* ist die Option *Cookie umschreiben* ebenfalls deaktiviert.

Host-Header durchreichen (optional): Wenn Sie diese Option wählen, bleibt der Host-Header (Kopfzeile) so erhalten, wie er vom Client angefragt wurde, und wird mit der Web-Anfrage an den Webserver weitergeleitet. Ob die Durchreichung des Host-Headers in Ihrer Umgebung notwendig ist, hängt jedoch von der Konfiguration Ihres Webservers ab.

4. **Klicken Sie auf *Speichern*.**
   Der Server wird der Liste *Virtuelle Webserver* hinzugefügt.

5. **Virtuellen Webserver aktivieren.**
   Der neue virtuelle Webserver ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler um den virtuellen Webserver zu aktivieren.

   Der virtuelle Webserver ist nun aktiviert (Schieberegler zeigt Grün).

In der Liste *Virtuelle Webserver* wird für jeden echten Webserver, der einem virtuellen Webserver zugeordnet ist, eine Statusampel angezeigt. Die Statusampel eines echten Webservers ist rot, wenn der echte Webserver nicht aktiviert wurde. Sie ist gelb, wenn der echte Webserver nicht hochgefahren oder nicht verfügbar ist, und grün, wenn alles einwandfrei funktioniert.

13.1.2 Echte Webserver

Auf der Registerkarte *Web Application Firewall > Echte Webserver* können Sie die Webserver hinzufügen, die durch die WAF geschützt werden sollen.

Um einen Webserver hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neuer echter Webserver*.**
   Das Dialogfeld *Echten Webserver anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den Webserver ein.

Host: Wählen Sie einen Host des Typs *Host* oder *DNS-Host* aus oder fügen Sie ihn hinzu. Es ist sehr empfehlenswert, hier den DNS-Hostnamen zu verwenden, weil Hosts, die mit ihrer IP-Adresse aufgeführt sind, leere Host-Header übermitteln, was bei manchen Browsern zu Problemen führen kann. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Art: Legen Sie für die Kommunikation zwischen UTM und dem Webserver *Verschlüsselt (HTTPS)* oder *Reiner Text (HTTP)* fest.

Port: Geben Sie eine Portnummer für die Kommunikation zwischen UTM und dem Webserver ein. Der Standard ist Port 80 bei *Reiner Text (HTTP)* und Port 443 bei *Verschlüsselt (HTTPS)*.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   HTTP-Keep-Alive verwenden: Standardmäßig verwendet die WAF HTTP-Keep-Alive, d. h., HTTP-persistente Verbindungen, wodurch Prozessor- und Speichernutzung reduziert werden. In den seltenen Fällen, in denen ein echter Webserver HTTP-Keep-Alive nicht korrekt unterstützt, kann diese Funktion Lesefehler oder Zeitüberschreitungen auslösen und sollte dann für den betreffenden Webserver ausgeschaltet werden. Wenn einem virtuellen Webserver zumindest ein echter Webserver zugeordnet ist, bei dem HTTP-Keep-Alive ausgeschaltet ist, wird die Funktion automatisch auch für alle anderen echten Webserver, die diesem virtuellen Webserver zugeordnet sind, ausgeschaltet.

4. **Klicken Sie auf *Speichern*.**
   Der Server wird der Liste *Echte Webserver* hinzugefügt.

Den vorhandenen Webservern können Sie jetzt auf der Registerkarte *Virtuelle Webserver* Firewall-Profile zuweisen.

13.1.3 Firewall-Profile

Auf der Registerkarte *Web Application Firewall > Firewall-Profile* können Sie WAF-Profile anlegen, die die Sicherheitsmodi und -stufen für Ihre Webserver festlegen.

Um ein WAF-Profil anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neues Firewall-Profil*.**
   Das Dialogfeld *Firewall-Profil anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für das Profil an.

   Outlook Anywhere durchlassen: Erlaubt externen Microsoft-Outlook-Clients den Zugriff auf den Microsoft Exchange Server über die WAF. Microsoft-Outlook-Verkehr wird nicht durch die WAF überprüft oder geschützt.

   Hinweis – Wenn Sie *Outlook Anywhere durchlassen* auswählen, werden die untenstehenden Bedingungen deaktiviert.

   Modus: Wählen Sie einen Modus aus der Auswahlliste:

   - **Überwachen:** HTTP-Anfragen werden überwacht und protokolliert.
   - **Ablehnen:** HTTP-Anfragen werden abgelehnt.

   Der gewählte Modus wird angewendet, sobald eine der unten gewählten Bedingungen auf eine HTTP-Anfrage zutrifft.

   Hinweis – Wenn Sie eine der untenstehenden Bedingungen auswählen, wird *Outlook durchlassen* deaktiviert.

   Filter für allgemeine Bedrohungen: Bei Aktivierung können Sie Ihre Webserver vor verschiedenen Bedrohungen schützen. Sie können die zu verwendenden Bedrohungsfilterkategorien unten im Abschnitt *Bedrohungsfilterkategorien* festlegen. Alle Anfragen werden gemäß den Regelwerken der ausgewählten Kategorien überprüft. Abhängig vom Ergebnis der Überprüfung wird ein Hinweis oder eine Warnung im Live-Protokoll angezeigt oder die Anfrage wird direkt blockiert.

      Strenge Filterung: Bei Aktivierung werden verschiedene der ausgewählten Regeln verschärft. Dies kann zu Falschmeldungen führen.

      Filterregeln übergehen: Manche der ausgewählten Bedrohungskategorien können Regeln enthalten, die zu Falschmeldungen führen. Um das Anzeigen von Falschmeldungen, die von einer bestimmten Regel generiert werden, zu vermeiden, fügen Sie die Nummer der zu überspringenden Regel in dieses Feld ein. Die WAF-Regel-Nummern können Sie beispielsweise auf der Seite

Protokollierung & Berichte > Webserver Protection > Details mithilfe des Filters *Häufigste Regeln* abrufen.

Cookie-Signierung: Schützt einen Webserver vor manipulierten Cookies. Wenn der Webserver einen Cookie setzt, wird ein zweiter Cookie zum ersten Cookie hinzugefügt, welcher einen Hash enthält, der aus dem Namen und dem Wert des ersten Cookies und einem Schlüssel besteht, wobei dieser Schlüssel nur der WAF bekannt ist. Wenn eine Anfrage nicht das richtige Cookie-Paar vorweisen kann, fand irgendeine Manipulation statt und der Cookie wird verworfen.

URL-Hardening: Schützt vor URL-Umschreibung. Dafür werden alle URLs einer Website signiert, sobald ein Client diese Website anfordert. Die Vorgehensweise bei der Signierung ähnelt derjenigen bei der Cookie-Signierung. Darüber hinaus wird die Antwort des Webservers im Hinblick darauf analysiert, welche Links als nächstes gültig angefordert werden können. Derartig „gefestigte“ URLs können des Weiteren als Lesezeichen abgespeichert und später besucht werden. Wählen Sie eine der folgenden Methoden, um Einstiegs-URLs zu definieren:

- **Manuell definierte Einstiegs-URLs:** Geben Sie URLs an, die als Einstiegs-URLs für eine Website dienen und deshalb nicht signiert werden müssen. Die Syntax muss einem der folgenden Beispiele entsprechen: `http://shop.beispiel.de/produkte/`, `https://shop.beispiel.de/produkte/` oder `/produkte/`.
- **Einstiegs-URLs von hochgeladener Google-Sitemap-Datei:** Sie können hier eine Sitemap-Datei hochladen, die Informationen zur Struktur Ihrer Website enthält. Sitemap-Dateien können im XML- oder Nur-Text-Format hochgeladen werden. Letzteres enthält lediglich eine URL-Liste. Sobald das Profil gespeichert ist, wird die Sitemap-Datei von der WAF geparst.
- **Einstiegs-URLs von Google-Sitemap-URL:** Sie können UTM eine Sitemap-Datei von einer vorgegebenen URL herunterladen lassen, die Informationen zur Struktur Ihrer Website enthält. Diese Datei kann regelmäßig auf Aktualisierungen überprüft werden.Sobald das Profil gespeichert ist, wird die Sitemap-Datei von der WAF heruntergeladen und geparst.

  URL: Geben Sie den Pfad zur Sitemap als absolute URL ein.

  Aktualisierung: Wählen Sie ein Aktualisierungsintervall aus dieser Auswahlliste. Wenn Sie *Manuell* wählen, wird die Sitemap nur aktualisiert, wenn Sie das Profil erneut speichern.

> **Hinweis –** Wenn Sie die Umkehrauthentifizierung mit dem Frontend-Modus *Formular* für den konfigurierten Pfad verwenden, ist es nicht nötig, eine Einstiegs-URL für die Anmeldung und den Pfad anzugeben. Wie man den Pfad konfiguriert ist auf der Seite *Webserver Protection* > *Web Application Firewall* > *Site-Path-Routing* beschrieben.

> **Hinweis –** URL-Hardening wird auf alle Dateien mit HTTP-Inhalt des Typs `text/*` oder `*xml*` angewandt (* dient als Platzhalter). Stellen Sie sicher, dass andere Dateitypen, z. B. Binärdateien, den richtigen HTTP-Inhaltstyp aufweisen, da sie sonst durch das URL-Hardening beschädigt werden können.

Form-Hardening: Schützt vor Umschreibung von Webformularen. Das Form-Hardening speichert die ursprüngliche Struktur eines Webformulars und fügt eine Signatur hinzu. Daher lehnt der Server die Anfrage ab, wenn sich die Struktur eines Formulars, das an den Server übermittelt wird, geändert hat.

> **Hinweis –** Form-Hardening wird auf alle Dateien mit HTTP-Inhalt des Typs `text/*` oder `*xml*` angewandt (* dient als Platzhalter). Stellen Sie sicher, dass andere Dateitypen, z. B. Binärdateien, den richtigen HTTP-Inhaltstyp aufweisen, da sie sonst durch das Form-Hardening beschädigt werden können.

Antivirus: Wählen Sie diese Option, um einen Webserver vor Viren zu schützen.

Modus: Sophos UTM bietet mehrere Antiviren-Mechanismen für höchste Sicherheit.

- **Einzelscan:** Standardeinstellung; bietet maximale Leistung. Die auf der Registerkarte *Systemeinstellungen* > *Scan-Einstellungen* festgelegte Engine wird verwendet.
- **Zweifachscan:** Bietet maximale Erkennungsrate, da der entsprechende Verkehr von zwei verschiedenen Virenscannern gescannt wird. Beachten Sie, dass Zweifachscan mit einem BasicGuard-Abonnement nicht verfügbar ist.

Richtung: Wählen Sie aus der Auswahlliste, ob nur Uploads, nur Downloads oder beide gescannt werden sollen.

Unscannbaren Inhalt blockieren: Wählen Sie diese Option, um Dateien zu blockieren, die nicht gescannt werden können. Der Grund hierfür kann unter anderem sein, dass Dateien verschlüsselt oder beschädigt sind.

Clients mit schlechtem Ruf blockieren: Anhand von GeoIP- und RBL-Informationen können Sie Clients blockieren, die laut ihrer Klassifizierung einen schlechten Ruf haben.Sophosverwendet folgende Klassifizierungsanbieter:

RBL-Quellen:

- Commtouch IP Reputation (ctipd.org)
- dnsbl.proxybl.org
- http.dnsbl.sorbs.net

Die GeoIP-Quelle ist Maxmind. Die WAF blockiert Clients, die in eine der folgenden Maxmind-Kategorien fallen:

- A1: Anonyme Proxies oder VPN-Dienste, die Clients nutzen, um ihre IP-Adressen oder ihren ursprünglichen geografischen Standort zu verschleiern.
- A2: Satellitenanbieter sind ISPs, die Benutzern auf der ganzen Welt Internetzugang über Satellit zur Verfügung stellen, oftmals von Hochrisiko-Ländern aus.

Keine Fernabfragen für Clients mit schlechtem Ruf: Da bei Fernabfragen auch Anfragen an entfernte Klassifizierungsanbieter gesendet werden müssen, kann die Verwendung von rufbasiertem Blockieren zu Leistungseinbußen Ihres Systems führen. Wählen Sie diese Option, um nur GeoIP-basierte Klassifizierung zu verwenden, bei der zwischengespeicherte Informationen zum Einsatz kommen, was die Geschwindigkeit deutlich erhöht.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Wählen Sie optional die folgenden Bedrohungsfilterkategorien aus** (nur verfügbar, wenn *Filter für allgemeine Bedrohungen* aktiviert ist):
   Protokollverletzungen: Erzwingt Erfüllung der RFC-Standard-Spezifikation des HTTP-Protokolls. Eine Verletzung dieser Standards ist üblicherweise ein Hinweis auf schädliche Inhalte.

Protokollanomalien: Sucht nach häufigen Nutzungsmustern. Das Fehlen solcher Muster weist häufig auf schädliche Anfragen hin. Zu solchen Mustern gehören z. B. HTTP-Header wie „Host“ oder „User-Agent“.

Grenzwerte anfragen: Erzwingt angemessene Grenzwerte für die Anzahl und den Bereich von Anfrageargumenten. Ein Überladen von Anfrageargumenten ist ein typischer Angriffsvektor.

HTTP-Richtlinie: Schränkt die zulässige Nutzung des HTTP-Protokolls ein. Webbrowser nutzen normalerweise nur eine begrenzte Untermenge aller möglichen HTTP-Optionen. Eine Untersagung der selten verwendeten Optionen schützt vor Angreifern, die auf solche oft weniger gut unterstützten Möglichkeiten abzielen.

Schädliche Roboter: Prüft auf Nutzungsmuster, wie sie für Bots und Crawler charakteristisch sind. Durch die Zugriffsverweigerung ist es unwahrscheinlicher, dass potenzielle Schwachstellen Ihrer Webserver entdeckt werden.

Generische Angriffe: Sucht nach versuchten Befehlsausführungen, welche die meisten Angriffe kennzeichnen. Nach einer Sicherheitsverletzung eines Webservers versucht ein Angreifer üblicherweise, auf dem Server Befehle auszuführen, wie z. B. Berechtigungen zu erweitern oder Datenspeicher zu manipulieren. Durch die Suche nach diesen Ausführungsversuchen, die nach einer Sicherheitsverletzung auftreten, können Angriffe erkannt werden, die anderenfalls möglicherweise unentdeckt geblieben wären, weil sie z. B. mit berechtigtem Zugriff einen verwundbaren Dienst anvisieren.

SQL-Injection-Angriffe: Sucht nach eingebetteten SQL-Befehlen und Escape-Zeichen in Anfrageargumenten. Die meisten Angriffe auf Webserver zielen auf Eingabefelder ab, die dazu verwendet werden können, eingebettete SQL-Befehle an die Datenbank zu richten.

(XSS-) Angriffe: Sucht nach eingebetteten Skripttags und Code in Anfrageargumenten. Mit Cross-Site-Scripting-Angriffen wird üblicherweise versucht, Skriptcode in Eingabefeldern auf einem Ziel-Webserver zu platzieren, häufig auf legitime Weise.

Hohe Sicherheit: Führt strikte Sicherheitsprüfungen für Anfragen durch, z. B. Prüfungen auf verbotene Pfad-Traversal-Versuche.

Trojaner: Prüft auf Nutzungsmuster, wie sie für Trojaner typisch sind, und sucht damit nach Anfragen, die eine Trojaneraktivität nahelegen. Die Funktion verhindert jedoch nicht die Installation solcher Trojaner; dafür sind die Antiviren-Scanner zuständig.

Ausgehend: Verhindert, dass Webserver Informationen an den Client durchlassen. Dazu gehören z. B. Fehlermeldungen, die von Servern gesendet werden und die Angreifer nutzen können, um vertrauliche Informationen zu erhalten oder bestimmte Schwachstellen zu erkennen.

4. **Klicken Sie auf *Speichern*.**
   Das WAF-Profil wird der Liste *Firewall-Profile* hinzugefügt.

Weitere Informationen zu URL-Hardening und Form-Hardening

Am besten wäre es, jederzeit sowohl URL-Hardening als auch Form-Hardening zu nutzen, da sich beide Funktionen gegenseitig ergänzen. Insbesondere verhindern Sie dadurch Probleme, die auftreten können, wenn Sie nur eine Option nutzen.

- Nur Form-Hardening ist aktiviert: Wenn eine Webseite Hyperlinks enthält, denen Anfragen angehängt sind (was bei bestimmten CMS der Fall ist), z. B. `http://beispiel.de/?view=article&id=1`, werden solche Seitenabfragen durch Form-Hardening blockiert, da die Signatur fehlt.
- Nur URL-Hardening ist aktiviert: Wenn ein Webbrowser Formulardaten an die Aktions-URL des `form`-Tags eines Webformulars anhängt (was bei GET-Anfragen der Fall ist), werden die Formulardaten in die Anfrage-URL integriert, die an den Webserver gesendet wird. Dadurch wird die URL-Signatur ungültig.

Diese Probleme treten nicht auf, wenn beide Funktionen aktiviert sind, da der Server die Anfrage akzeptiert, wenn entweder Form-Hardening oder URL-Hardening die Anfrage für gültig befindet.

Outlook Web Access

Die Konfiguration der WAF für Outlook Web Access (OWA) ist etwas heikel, da OWA Anfragen von einer öffentlichen IP anders behandelt als interne Anfragen von einer internen LAN-IP an die OWA-Website. Es gibt Umleitungen (engl. redirects), die an die OWA-URLs angehängt werden, wobei bei externem Zugriff die externe FQDN verwendet wird, bei internen Anfragen hingegen die interne Server-IP-Adresse.

Zur Lösung muss das OWA-Verzeichnis als *Einstiegs-URL* im WAF-Profil Ihres OWA-Webservers eingetragen werden (z. B. `http://webserver/exchange/`). Zusätzlich müssen Sie eine Ausnahme anlegen, die URL-Hardening für den Pfad `/exchange/*` ausnimmt, und Sie müssen die Cookie-Signierung für den virtuellen Server komplett ausschalten.

13.1.4 Ausnahmen

Auf der Registerkarte *Web Application Firewall > Ausnahmen* können Sie Webanfragen oder Quellnetzwerke definieren, die von bestimmten Prüfungen ausgenommen sein sollen.

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmenliste*.**
   Das Dialogfeld *Ausnahmenliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Ausnahme ein.

   Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen aus, die nicht durchgeführt werden sollen. Beschreibungen finden Sie unter *Firewall-Profile*.

   Diese Kategorien überspringen: Wählen Sie die Bedrohungsfilterkategorien aus, die aufgehoben werden sollen. Beschreibungen finden Sie unter *Firewall-Profile*.

   Virtuelle Webserver: Wählen Sie die virtuellen Webserver aus, die von den ausgewählten Prüfungen ausgenommen werden sollen.

   Für alle Anfragen: Wählen Sie aus der Auswahlliste eine Anfragedefinition aus. Beachten Sie, dass Sie zwei Anfragedefinitionen durch entweder „und“ oder „oder“ logisch kombinieren können.

      Netzwerke: Wählen Sie die Quellnetzwerke, aus denen die Client-Anfragen stammen und die von den gewählten Prüfungen ausgenommen werden sollen, aus oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

      Pfade: Fügen Sie die Pfade, die von den gewählten Prüfungen ausgenommen werden sollen, z. B. in der Form `/produkte/bilder/*` hinzu.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   HTML während URL-Hardening oder Form-Hardening nie ändern: Wenn diese Option ausgewählt ist, werden keine Daten, die mit den festgelegten Ausnahmeeinstellungen übereinstimmen, von der WAF-Engine geändert. Mit dieser Option werden beispielsweise Binärdaten, die vom echten Webserver fälschlicherweise mit dem Inhaltstyp text/html bereitgestellt wurden, nicht beschädigt. Andererseits können Webanfragen blockiert werden, wenn URL-Hardening, HTML-Umschreibung oder Form-

Hardening aktiviert ist. Diese drei Funktionen nutzen einen HTML-Parser und hängen daher bis zu einem gewissen Grad von der Änderung von Webseiten-Inhalten ab. Um unerwünschtes Blockieren zu vermeiden, überspringen Sie URL- bzw. Form-Hardening bei Anfragen, die von der Blockade betroffen sind. Möglicherweise müssen Sie dies aufgrund von Abhängigkeiten zwischen Webservern bzw. Webseiten in einer weiteren/neuen Ausnahme umsetzen.

4. **Klicken Sie auf *Speichern*.**
   Die neue Ausnahme wird in der Liste *Ausnahmen* angezeigt.

5. **Aktivieren Sie die Ausnahme.**
   Die neue Ausnahme ist standardmäßig deaktiviert (Schieberegler ist grau). Klicken Sie auf den Schieberegler um die Ausnahme zu aktivieren.

   Die Ausnahme ist jetzt aktiv (Schieberegler ist grün).

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

13.1.5 Site-Path-Routing

Auf der Registerkarte *Web Application Firewall > Site-Path-Routing* können Sie festlegen, an welche echten Webserver empfangene Anfragen weitergeleitet werden sollen. Sie können beispielsweise festlegen, dass alle URLs mit einem bestimmten Pfad, z. B. `/products` an einen bestimmten Webserver weitergeleitet werden. Sie können auch mehr als einen Webserver für eine bestimmte Anfrage konfigurieren und anhand von Regeln festlegen, wie die Anfragen an die Server verteilt werden sollen. Sie können beispielsweise auch festlegen, dass jede Sitzung während ihrer gesamten Dauer an einen bestimmten Webserver gebunden ist (permanente Sitzung, engl. sticky session). Dies ist beispielsweise erforderlich, wenn Sie einen Online-Shop betreiben und sicherstellen möchten, dass ein Kunde während eines Einkaufs immer mit demselben Server verbunden ist. Sie können auch einstellen, dass alle Anfragen an einen Webserver gesendet werden und die anderen nur als Backup dienen.

Für jeden virtuellen Webserver wird automatisch eine Standard-Site-Path-Route (mit Pfad `/`) erstellt. UTM wendet die Site-Path-Regeln automatisch in logischer Reihenfolge an: vom strengsten, d. h. längsten Pfad, bis hin zum Standard-Pfad, der nur verwendet wird, wenn kein anderer, spezifischerer Site-Path auf die erhaltene Anfrage zutrifft. Die Reihenfolge der Site-Path-Routen in der Liste spielt keine Rolle. Wenn keine Route auf eine erhaltene Anfrage zutrifft, z. B. weil die Standard-Route gelöscht wurde, wird die Anfrage abgelehnt.

> **Hinweis –** Der Zugriff auf die Registerkarte *Site-Path-Routing* ist erst möglich, wenn mindestens ein echter und ein virtueller Webserver erstellt wurden.

Um eine Site-Path-Route anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neue Site-Path-Route*.**
   Das Dialogfeld *Site-Path-Route erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Site-Path-Route ein.

   Virtueller Webserver: Wählen Sie den ursprünglichen Zielhost des eingehenden Datenverkehrs.

   Pfad: Geben Sie den Pfad ein, für den Sie die Site-Pfad-Route erstellen möchten, z. B. `/products`.

   Umkehrauthentifizierung: Wählen Sie das Authentifizierungsprofil mit den Benutzern oder Gruppen aus, die Zugang zu dieser Site-Path-Route haben sollen. Wenn kein Profil ausgewählt ist, ist keine Authentifizierung erforderlich.

   > **Achtung –** Bei Verwendung eines Umkehrauthentifizierungsprofils auf einem virtuellen Webserver, der im Klartextmodus ausgeführt wird, sind die Benutzerzugangsdaten offen sichtbar. Beim Fortfahren überträgt die Web Application Firewall Benutzerzugangsdaten auf unsichere Weise.

   > **Achtung –** Ein Authentifizierungsprofil mit dem Frontend-Modus *Formular* kann nur einmal auf einem bestimmten virtuellen Webserver implementiert werden.

   Echte Webserver: Aktivieren Sie die Auswahlkästchen vor den echten Webservern, die dem jeweiligen Pfad zugeordnet sind. Die Reihenfolge der ausgewählten Server ist nur für die Option *Hot-Standby-Modus aktivieren* relevant. Mit den Sortiersymbolen können Sie die Reihenfolge ändern.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Permanenten Sitzungscookie aktivieren: Wählen Sie diese Option, um sicherzustellen, dass jede Sitzung an einen echten Webserver gebunden ist. Wenn diese Option ausgewählt ist, wird ein Cookie im Browser des Benutzers abgelegt. Daraufhin leitet UTM alle Anfragen von diesem Browser an denselben echten Webserver weiter. Wenn der Server nicht verfügbar ist, wird das Cookie aktualisiert und die Sitzung wechselt auf einen anderen Webserver.

   Hot-Standby-Modus aktivieren: Wählen Sie diese Option aus, wenn alle Anfragen an den ersten ausgewählten echten Webserver gesendet werden und die anderen Webserver nur als Backup dienen sollen. Die Backup-Server kommen nur zum Einsatz, wenn der Hauptserver ausfällt.Sobald der Hauptserver wieder in Betrieb ist, wechseln die Sitzungen wieder zum Hauptserver, es sei denn, Sie haben die Option *Permanenten Sitzungscookie aktivieren* ausgewählt.

4. **Klicken Sie auf *Speichern*.**
   Die Site-Path-Route wird zur Liste *Site-Path-Routing* hinzugefügt.

Um eine Site-Path-Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

13.1.6 Erweitert

Auf der Registerkarte *Web Application Firewall > Erweitert* können Sie die Schlüssel definieren, die für die Cookie-Signierung und das URL-Hardening verwendet werden.

Cookie-Signierung

Hier können Sie einen eigenen Schlüssel angeben, der als Signaturschlüssel für die Cookie-Signierung verwendet wird.

URL-Hardening

Hier können Sie einen eigenen Schlüssel angeben, der als Signaturschlüssel für das URL-Hardening verwendet wird.

Form-Hardening

Hier können Sie einen eigenen Schlüssel angeben, der als Verschlüsselungsschlüssel für das Form-Hardening-Token verwendet wird.Der Schlüssel muss aus mindestens acht Zeichen bestehen.

13.2 Umkehrauthentifizierung

Auf den Seiten *Webserver Protection > Umkehrauthentifizierung* können Sie definieren, wie die Web Application Firewall verwendet wird, um Benutzer direkt zu authentifizieren, anstatt die Authentifizierung den echten Webservern zu überlassen. Über Authentifizierungsprofile kann die Umkehrauthentifizierung verwendet werden, um bestimmte Authentifizierungseinstellungen jeder Site-Path-Route zuzuweisen.

Ein Authentifizierungsprofil wird im Wesentlichen durch zwei Authentifizierungsmodi definiert: der Authentifizierungsmodus, der zwischen dem Benutzer und der WAF verwendet wird, und der Authentifizierungsmodus, der zwischen der WAF und den echten Webservern verwendet wird. Wenn ein echter Webserver keine Authentifizierung unterstützt, kann die WAF daher die Authentifizierung der Benutzer erzwingen. Auf der anderen Seite stellt die Umkehrauthentifizierung sicher, dass sich ein Benutzer nur einmal authentifizieren muss, selbst wenn dem jeweiligen virtuellen Webserver mehr als ein echter Webserver zugewiesen ist.

Wenn Sie Formulare für die Benutzerauthentifizierung verwenden, können sie unternehmensspezifische Formularvorlagen verwenden.

13.2.1 Profile

Auf der Registerkarte *Webserver Protection > Umkehrauthentifizierung > Profile* legen Sie die Authentifizierungsprofile für die Web Application Firewall fest. Mit Profilen können Sie unterschiedlichen Benutzern oder Benutzergruppen unterschiedliche Authentifizierungseinstellungen zuweisen. Nach Festlegung der Authentifizierungsprofile können Sie diese den Site-Path-Routen auf der Registerkarte *Web Application Firewall > Site-Path-Routing* zuweisen.

Um ein Authentifizierungsprofil hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Profile* auf *Neues Authentifizierungsprofil*.**
   Das Dialogfeld *Authentifizierungsprofil erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für das Profil an.

   Frontend-Modus: Wählen Sie die Authentifizierungsmethode der Benutzer für die Web Application Firewall aus.

Einfach: Die Authentifizierung erfolgt mittels einfacher HTTP-Authentifizierung mit Eingabe von Benutzernamen und Kennwort. Da die Zugangsdaten in diesem Modus unverschlüsselt übertragen werden, sollte er in Verbindung mit HTTPS genutzt werden. In diesem Modus werden keine Sitzungs-Cookies generiert und eine dedizierte Abmeldung ist nicht möglich.

Formularvorlage: Benutzern wird ein Formular angezeigt, in das sie ihre Zugangsdaten eingeben müssen. In diesem Modus werden Sitzungs-Cookies generiert und eine dedizierte Abmeldung ist möglich. Die zu verwendende Formularvorlage können Sie über die Auswahlliste *Formularvorlage* auswählen. Neben der Standardformularvorlage sind die Formulare aufgelistet, die auf der Registerkarte *Formularvorlagen* definiert wurden.

Frontend-Bereich: Der Bereich ist eine eindeutige Zeichenfolge, die zur Definition des Pfads zum URL-Authentifizierungsformular. Es ist wichtig, eine Zeichenfolge einzugeben, die nicht als Pfad auf dem zugehörigen echten Webserver verwendet wird. Andernfalls können die Benutzer nicht auf den Pfad des echten Webservers zugreifen.

Hinweis – Diese Zeichen sind für den *Frontend-Bereich* zulässig: A–Z a–z 0–9 , ; . : - _ # ' + =) (& % $! ^ < > | @

Formularvorlage: Wählen Sie die Vorlage, die den Benutzern für die Authentifizierung angezeigt wird. Formularvorlagen werden auf der Seite *Formularvorlagen* definiert.

Backend-Modus: Wählen Sie die Authentifizierungsart der Web Application Firewall für echte Webserver aus. Der Backend-Modus muss mit den Authentifizierungseinstellungen des echten Webservers übereinstimmen.

Einfach: Die Authentifizierung erfolgt mittels einfacher HTTP-Authentifizierung mit Eingabe von Benutzernamen und Kennwort.

Keine: Es erfolgt keine Authentifizierung zwischen der WAF und den echten Webservern. Beachten Sie, dass die Benutzerauthentifizierung im Frontend-Modus erfolgt, wenn Ihre echten Webserver keine Authentifizierung unterstützen.

Benutzer/Gruppen: Wählen Sie die Benutzer oder Benutzergruppen aus, die diesem Authentifizierungsprofil zugewiesen werden sollen. Nachdem dieses Profil einer Site-Path-Route zugewiesen wurde, haben diese Benutzer Zugriff auf den Site-Path mit den Authentifizierungseinstellungen, die in diesem Profil definiert sind. Normalerweise

handelt es sich dabei um eine Backend-Benutzergruppe. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* erläutert.

> **Hinweis –** In einigen Fällen ist es sinnvoll, wenn Benutzer sich an die Benutzer-Prinzipalnamenotation halten müssen (user@domain), wenn Sie Ihre Daten eingeben. Zum Beispiel, wenn man Exchange-Server in Kombination mit Active-Directory-Servern verwendet. Nähere Informationen zur Verwendung der Notation finden Sie unter *Definitionen & Benutzer > Authentifizierungsdienste > Server* im Bereich *Active Directory*.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Sitzungs-Zeitüberschreitung aktivieren: zur Beschränkung der Sitzung.

   Sitzungs-Zeitüberschreitung: zur Festlegung des Zeitwerts.

   Zeitüberschreitung in: zur Festlegung des Zeitraums in *Tagen*, *Stunden* oder *Minuten*.

   Sitzungsdauer beschränken: zur Beschränkung der Sitzungsdauer.

   Sitzungsdauer: zur Festlegung der Dauer.

   Sitzungsdauer in: zur Festlegung des Zeitraums in *Tagen*, *Stunden* oder *Minuten*.

> **Hinweis –** Der *Cookie-Verschlüsselungsschlüssel* wird angezeigt, wenn für den *Frontend-Modus* die Option *Formular* ausgewählt wurde.

4. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**
   Sitzungs-Zeitüberschreitung aktivieren: Wählen Sie diese Option, um eine Zeitbeschränkung für die Benutzersitzung zu aktivieren. Dadurch müssen die Benutzerzugangsdaten durch erneutes Anmelden bestätigt werden, wenn Benutzer auf dem virtuellen Webserver längere Zeit keine Aktionen durchführen.

   Sitzungs-Zeitüberschreitung: Legen Sie ein Intervall für die Sitzungs-Zeitüberschreitung fest.

Zeitüberschreitung in: Legen Sie die Einheit für die Sitzungs-Zeitüberschreitung fest.

Sitzungsdauer beschränken: Wählen Sie diese Option, um eine feste Beschränkung der Zeitdauer zu bestimmen, die Benutzer unabhängig von den durchgeführten Aktivitäten angemeldet bleiben dürfen.

Sitzungsdauer: Legen Sie ein Intervall für die Beschränkung der Sitzungsdauer fest.

Sitzungsdauer in: Legen Sie die Einheit für die Sitzungsdauer fest.

Cookie-Verschlüsselungschlüssel: zur Festlegung des Schlüssels für die Cookie-Verschlüsselung.

> **Hinweis –** Der *Cookie-Verschlüsselungsschlüssel* ist nur verfügbar, wenn im Authentifizierungsprofil für den *Frontend-Modus* die Option *Formular* festgelegt wurde.

Einfache Authentifizierung entfernen: zur Weiterleitung des Authentication Header *Authorize* für die einfache Authentifizierung, damit doppelschichtige HTTP-Authentifizierung verwendet werden kann. Aktivieren Sie die Checkbox um die Basisauthentifizierung zu überspringen.

> **Hinweis –** *Einfache Authentifizierung entfernen* ist nur verfügbar, wenn der *Backend-Modus* im Authentifizierungsprofil auf *keine* steht.

> **Achtung –** Bei Verwendung von Umkehrauthentifizierung in Verbindung mit OTP werden die OTP-Token nur einmal bei der Einrichtung einer Benutzersitzung überprüft. Nach der Einrichtung der Sitzung erfolgt bei darauffolgenden Anmeldungen desselben Benutzers keine Überprüfung der OTP-Token. Dies erfolgt aus dem Grund, dass böswillige Benutzer möglicherweise die OTP-Konfiguration mit unzähligen Authentifizierungsanforderungen für die geschützten Pfade überfluten können. Dadurch würden OTP-Prüfungen erzeugt und auf den Authentifizierungs-Daemon ein erfolgreicher DoS-Angriff gestartet. Kennwörter und andere Anforderungsaspekte werden aber weiterhin für den Abgleich der Konfiguration überprüft.

5. **Klicken Sie auf *Speichern*.**
   Das neue Profil wird in der Liste *Profile* angezeigt.

Um ein Profil zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

13.2.2 Formularvorlagen

Auf der Registerkarte *Webserver Protection > Umkehrauthentifizierung > Formularvorlagen* können Sie HTML-Formulare für die Umkehrauthentifizierung hochladen. Eine Formularvorlage kann mit dem Frontend-Modus *Formular* einem Authentifizierungsprofil zugewiesen werden. Das jeweilige Formular wird präsentiert, wenn ein Benutzer versucht, auf einen Site-Path zuzugreifen, dem das Authentifizierungsprofil zugewiesen ist.

Um eine Formularvorlage hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Formularvorlagen* auf *Neue Formularvorlage*.**
   Das Dialogfenster *Neue Formularvorlage erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für die Formularvorlage ein.

   Dateiname: Klicken Sie auf das Ordnersymbol, um die HTML-Vorlage auszuwählen und hochzuladen.

   Bilder/Stylesheets: Wählen Sie die Bilder, Stylesheets oder JavaScript-Dateien, die von der ausgewählten Formularvorlage verwendet werden aus und laden Sie sie hoch.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.
3. **Klicken Sie auf *Speichern*.**
   Die neue Formularvorlage wird in der Liste *Formularvorlagen* angezeigt.

Um eine Formularvorlage zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

13.3 Zertifikatverwaltung

Über das Menü *Webserver Protection > Zertifikatverwaltung*, das dieselben Konfigurationsoptionen enthält wie das Menü *Site-to-Site-VPN > Zertifikatverwaltung*, können Sie alle zertifikatbezogenen Vorgänge von Sophos UTM verwalten. Das beinhaltet unter anderem das Anlegen und Importieren von X.509-Zertifikaten sowie das Hochladen sogenannter *Zertifikatsperrlisten* (CRLs).

13.3.1 Zertifikate

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Zertifikate*.

13.3.2 Certificate Authority (Zertifizierungsstelle)

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *CA*.

13.3.3 Sperrlisten (CRLs)

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Sperrlisten (CRLs)*.

13.3.4 Erweitert

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Erweitert*.

14 RED-Verwaltung

In diesem Kapitel wird beschrieben, wie Sie Sophos RED konfigurieren. RED ist die Abkürzung für *Remote Ethernet Device* (entferntes Ethernet-Gerät) und bezeichnet eine Methode, räumlich getrennte Zweigniederlassungen und dergleichen so mit Ihrer Hauptniederlassung zu verbinden, als ob die Zweigniederlassung Teil Ihres lokalen Netzwerks sei.

Der Aufbau besteht aus einer Sophos UTM in Ihrer Hauptniederlassung und einem Remote Ethernet Device (RED) in Ihrer Zweigniederlassung. Die Herstellung einer Verbindung zwischen den beiden ist ausgesprochen einfach, da die RED-Appliance selbst nicht konfiguriert werden muss. Sobald die RED-Appliance mit Ihrer UTM verbunden ist, verhält sie sich wie jedes andere Ethernet-Gerät auf Ihrer UTM. Aller Verkehr Ihrer Zweigstelle wird sicher über Ihre UTM geroutet, das bedeutet, dass Ihre Zweigniederlassung so gesichert ist wie Ihr lokales Netzwerk.

Aktuell stehen zwei Typen von RED-Appliances zur Verfügung:

- RED 10: RED-Lösung für kleine Zweigniederlassungen
- RED 50: RED-Lösung mit zwei Uplink-Schnittstellen für größere Zweigniederlassungen.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Übersicht
- Allgemein
- Clientverwaltung
- Einrichtungshilfe
- Tunnelverwaltung

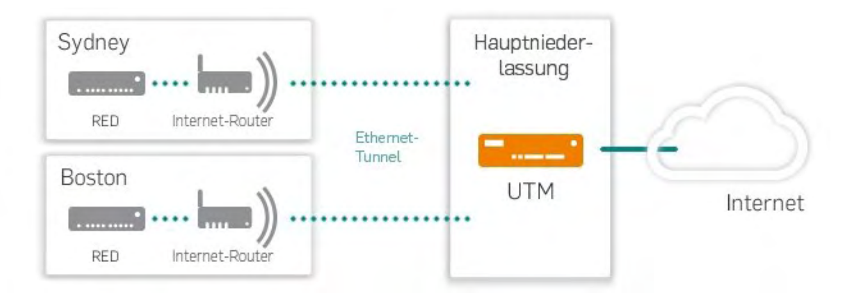


Bild 24 RED: Aufbaukonzept

Der Aufbau einer RED-Umgebung umfasst die folgenden Schritte:

1. Aktivierung der RED-Unterstützung.
2. Konfiguration der RED-Appliance auf Ihrer UTM.
3. Verbindung der RED-Appliance mit dem Internet am entfernten Standort.

Hinweis – Die Übersichtsseite von RED zeigt allgemeine Informationen zur RED-Architektur, solange noch keine RED-Appliance konfiguriert ist. Wenn eine RED-Appliance konfiguriert wurde, zeigt die Seite Informationen zum Status von RED.

14.1 Übersicht

Die Seite *Übersicht* bietet allgemeine Informationen darüber, wofür RED gedacht ist, wie es funktioniert und wie ein typischer Einsatz von RED aussieht.

Querverweis – Weitere Informationen über RED-Appliances finden Sie in den *Quick-Start-Guides* und *Hinweisen zum Betrieb* im Sophos UTM-Resource-Center. Die LED-Blink-Codes der RED-10-Appliances sind in der Sophos-Knowledgebase beschrieben.

RED-Live-Protokoll öffnen

Sie können das Live-Protokoll verwenden, um die Verbindung zwischen Ihrer Sophos UTM und der RED-Appliance zu überwachen. Klicken Sie auf die Schaltfläche *RED-Live-Protokoll öffnen*, um das Live-Protokoll in einem neuen Fenster zu öffnen.

14.2 Allgemeine Einstellungen

Auf der Registerkarte *Allgemeine Einstellungen* können Sie die Unterstützung für RED ein- oder ausschalten, das heißt, ob UTM als RED-Hub agiert.Sie müssen die RED-Unterstützung einschalten, bevor eine RED-Appliance eine Verbindung mit UTM herstellen kann.

RED-Konfiguration

Um die RED-Unterstützung zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die RED-Unterstützung auf der Registerkarte *Allgemeine Einstellungen*.**

Klicken Sie auf den Schieberegler.

Der Schieberegler wird gelb und der Abschnitt *RED-Hub-Konfiguration* kann nun bearbeitet werden.

2. **Geben Sie Informationen zu Ihrer Organisation ein.**
   Standardmäßig werden die Einstellungen von der Registerkarte *Verwaltung* > *Systemeinstellungen* > *Organisatorisches* verwendet.

3. **Klicken Sie auf *RED aktivieren*.**
   Der Schieberegler wird grün und die RED-Unterstützung ist aktiv.UTM registriert sich nun beim RED Provisioning Service (RPS) von Sophos, um als RED-Hub zu agieren.

   Sie können nun fortfahren, indem Sie eine oder mehrere RED-Appliances auf der Seite *Clientverwaltung* hinzufügen oder den Assistenten auf der Seite *Einrichtungshelfer* verwenden.

Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

Appliances automatisch Autorisierung entziehen

Wenn die RED-Unterstützung aktiv ist, können Sie festlegen, ob nicht verbundenen RED-Appliances automatisch nach einer bestimmten Zeitspanne die Autorisierung entzogen werden soll.Mit Hilfe dieser Funktion können Sie verhindern, dass sich gestohlene RED-Appliances mit UTM verbinden können.

Hinweis –Die Option *Appliances automatisch Autorisierung entziehen* funktioniert nicht für RED-Tunnel zwischen 2 UTMs.

1. **Aktivieren Sie die Funktion zur automatischen Entziehung der Autorisierung.**
   Wählen Sie das Auswahlkästchen *Automatisch Autorisierung entziehen*.

2. **Legen Sie eine Zeitspanne fest, nach der der RED-Appliance automatisch die Autorisierung entzogen wird.**
   Geben Sie den gewünschten Wert in das Feld *Nach* ein. Die kleinste mögliche Zeitspanne beträgt 5 Minuten.

3. **Klicken Sie auf *Übernehmen*.**
   Die Funktion „Automatisch Autorisierung entziehen“ ist jetzt aktiv.

Wenn sich eine RED-Appliance wieder verbinden möchte, nachdem sie länger als die definierte Zeitspanne nicht verbunden war, wird sie automatisch deaktiviert. Dies ist an den Schiebereglern auf der Seite *Clientverwaltung* zu erkennen. Auf der Seite *Übersicht* wird auch eine

entsprechende Warnung angezeigt. Um einer RED-Appliance, deren Autorisierung entzogen wurde, die Verbindung wieder zu erlauben, aktivieren Sie sie auf der Seite *Clientverwaltung*.

14.3 Clientverwaltung

Auf der Seite *RED-Verwaltung > Clientverwaltung* können Sie die Verbindung von entfernten UTMs mit Ihrer UTM über einen Remote Ethernet Device (RED)-Tunnel aktivieren. Die entfernten UTMs fungieren dann einfach als RED-Appliances. Darüber hinaus können Sie RED-Appliances manuell konfigurieren (Expertenmodus), anstatt die Einrichtungshilfe zu verwenden. Die Einrichtungshilfe ist ein bequemerer Weg, RED-Appliances zu konfigurieren, und befindet sich auf der nächsten WebAdmin-Seite.

Jede RED-Appliance oder jede UTM, die hier konfiguriert ist, kann eine Verbindung zu Ihrer UTM herstellen.

Die Markierung *[Server]* vor dem Seitennamen gibt an, dass diese Seite nur konfiguriert werden muss, wenn die UTM als Server (RED-Hub) fungieren soll.

Hinweis – Damit sich RED-Appliances verbinden können, müssen Sie zunächst die RED-Unterstützung auf der Seite *Allgemeine Einstellungen* aktivieren.

Einrichten eines RED-Tunnels zwischen zwei UTMs

Damit eine weitere UTM über einen RED-Tunnel eine Verbindung mit Ihrer lokalen UTM herstellen kann, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Clientverwaltung* auf *RED hinzufügen*.**
   Das Dialogfenster *RED hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Zweigstelle: Geben Sie einen Namen für die Zweigstelle ein, in der sich die Client-UTM befindet, z. B. „Büro München“.

   Client-Typ: Wählen Sie *UTM* aus der Auswahlliste aus.

   Tunnel-ID: Standardmäßig ist *Automatisch* ausgewählt. Tunnel werden durchnummeriert.Sie müssen sicherstellen, dass die Tunnel-ID beider UTMs eindeutig ist. In diesem Fall kann es erforderlich sein, eine andere ID aus der Auswahlliste auszuwählen.

3. **Klicken Sie auf *Speichern*.**

Das UTM-Objekt wird erstellt.

4. **Laden Sie die Bereitstellungsdatei herunter.**
   Um der entfernten (Client-)UTM die Konfigurationsdaten bereitzustellen, laden Sie die Bereitstellungsdatei mit Hilfe der Schaltfläche *Download* herunter und übertragen Sie die Datei auf sichere Weise zur entfernten UTM.

Konfiguration einer RED-Appliance

Um eine RED-Appliance mit Ihrer lokalen UTM zu verbinden, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Clientverwaltung* auf *RED hinzufügen*.**
   Das Dialogfenster *RED hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Zweigstelle: Geben Sie einen Namen für die Zweigstelle ein, in der sich das RED-Gerät befindet, z. B. „Büro München".

   Client-Typ: Wählen Sie *RED 10* oder *RED 50* aus der Auswahlliste, je nachdem, mit welchem RED-Typ Sie eine Verbindung herstellen möchten.

   > **Hinweis –** Die RED 50-Appliance verfügt über ein LCD-Display. Sie können sie verwenden, um wichtige Informationen zum Gerät anzuzeigen. Mit der Schaltfläche „Nach links" können Sie das Menü aufrufen. Navigieren Sie mit den Schaltflächen „Nach oben" bzw. „Nach unten" und verwenden Sie die Schaltfläche „Nach rechts" als Eingabetaste.Weitere Informationen finden Sie in den Hinweisen zum Betrieb.

   RED ID: Geben Sie die ID des RED-Geräts ein, das Sie gerade konfigurieren. Diese ID finden Sie auf der Rückseite der RED-Appliance und auf deren Verpackung.

   Tunnel-ID: Standardmäßig ist *Automatisch* ausgewählt. Tunnel werden durchnummeriert. Wenn Sie IDs haben, die miteinander in Konflikt stehen, wählen Sie eine andere ID aus der Auswahlliste aus.

   Entsperrcode (optional): Lassen Sie dieses Feld bei der ersten Einrichtung einer RED-Appliance leer. In dem Fall, dass die RED-Appliance, die Sie konfigurieren wollen, zuvor bereits einmal eingerichtet wurde, benötigen Sie deren Entsperrcode. Der Entsperrcode wird während der Einrichtung einer RED-Appliance erzeugt und sofort zu der Adresse gesendet, die auf der Registerkarte *Allgemeine Einstellungen* festgelegt ist. Dabei han-

delt es sich um eine Sicherheitsfunktion, die dafür sorgt, dass eine RED-Appliance nicht einfach entfernt und woanders installiert werden kann.

Hinweis – Für die manuelle Einrichtung über USB-Stick und die automatische Einrichtung mittels RED Provisioning Service (siehe unten) werden zwei verschiedene Entsperrcodes erzeugt. Wenn Sie bei einem RED-Gerät von einer Einrichtungsmethode zu einer anderen wechseln, stellen Sie sicher, dass Sie den entsprechenden Entsperrcode verwenden: Geben Sie bei einer manuellen Einrichtung den Entsperrcode der letzten manuellen Einrichtung ein; geben Sie bei einer automatischen Einrichtung den Entsperrcode der letzten automatischen Einrichtung ein.

Wenn Sie nicht im Besitz des Entsperrcodes sind, ist der einzige Weg, die RED-Appliance zu entsperren, den Sophos-Support zu kontaktieren. Der Support kann Ihnen jedoch nur dann helfen, wenn Sie die automatische RED-Einrichtung über den Sophos-RED-Provisioning-Service verwendet haben.

Tipp – Der Entsperrcode ist auch in Backup-Dateien der UTM enthalten, mit der das RED verbunden war, wenn das Backup hostspezifische Daten enthält.

UTM-Hostname: Sie müssen eine öffentliche IP-Adresse oder einen Hostnamen eingeben, über den der Zugriff auf Ihre UTM möglich ist.

2. UTM-Hostname: Für RED 50-Appliances können Sie eine weitere öffentliche IP-Adresse oder einen anderen Hostnamen derselben UTM eingeben. Beachten Sie, dass Sie keine IP-Adressen oder Hostnamen einer anderen UTM eingeben können.

Verwende 2. Hostnamen für (nur mit RED 50, siehe Abbildungen unten): Sie können festlegen, wofür der zweite Hostname verwendet werden soll.

- **Failover:** Wählen Sie diese Option, wenn Sie den zweiten Hostnamen nur für den Fall verwenden möchten, dass der erste Hostname ausfällt.
- **Lastverteilung:** Wählen Sie diese Option, um aktive Lastverteilung zwischen den beiden Hostnamen zu aktivieren. Dies ist sinnvoll, wenn die beiden Uplinks, mit denen die Hostnamen korrelieren, in Latenz und Durchsatz gleichwertig sind.

Uplink-Modus/2. Uplink-Modus: Sie können festlegen, wie das RED-Gerät eine IP-Adresse erhält, entweder über DHCP oder indem Sie ihm direkt eine statische IP-Adres-

se zuweisen. Für RED 50-Appliances legen Sie den Uplink-Modus jedes RED-Uplink-Ethernet-Anschlusses separat fest.

- **DHCP-Client:** Die RED-Appliance bezieht eine IP-Adresse von einem DHCP-Server.
- **Statische Adresse:** Geben Sie eine IPv4-Adresse, eine entsprechende Netzmaske, ein Standardgateway und einen DNS-Server ein.

Hinweis – Es existiert keine eindeutige Zuordnung zwischen UTM-Hostnamen und RED-Uplink-Ethernet-Anschlüssen.Jeder RED-Anschluss versucht, eine Verbindung mit jedem definierten UTM-Hostnamen herzustellen.

Verwende 2. Uplink für (nur mit RED 50, siehe Abbildungen unten): Sie können festlegen, wofür der zweite Uplink verwendet werden soll.

- **Failover:** Wählen Sie diese Option, wenn Sie den zweiten Uplink nur für den Fall verwenden möchten, dass der erste Uplink ausfällt.
- **Lastverteilung:** Wählen Sie diese Option, um aktive Lastverteilung zwischen den beiden Uplinks zu aktivieren. Dies ist sinnvoll, wenn die beiden Uplinks der RED 50-Appliance in Latenz und Durchsatz gleichwertig sind.

Betriebsmodus: Sie können festlegen, wie das entfernte Netzwerk in Ihr lokales Netzwerk integriert werden soll.

- **Standard/Vereint:** Die UTM kontrolliert den Netzwerkverkehr des entfernten Netzwerks vollständig. Darüber hinaus agiert sie als DHCP-Server und als Standardgateway. Das Routing des gesamten Netzwerkverkehrs des entfernten Netzwerks erfolgt über die UTM.
- **Standard/Getrennt:** Die UTM kontrolliert den Netzwerkverkehr des entfernten Netzwerks vollständig. Darüber hinaus agiert sie als DHCP-Server und als Standardgateway. Im Gegensatz zum vereinten Modus wird nur bestimmter Verkehr über die UTM geroutet. Legen Sie unten im Feld *Getrennte Netzwerke* lokale Netzwerke fest, auf die entfernte Clients Zugriff haben sollen.

  Hinweis – VLAN-getaggte Datenframes können mit diesem Betriebsmodus nicht bearbeitet werden. Wenn Sie hinter Ihrer RED-Appliance ein VLAN verwenden, arbeiten Sie stattdessen im *Standard*-Modus.

- **Transparent/Getrennt:** Die UTM kontrolliert weder den Netzwerkverkehr des entfernten Netzwerks, noch fungiert sie als DHCP-Server oder als Standardgateway. Im Gegenteil, sie bezieht eine IP-Adresse vom DHCP-Server des entfernten Netzwerks, um ein Teil von jenem Netzwerk zu werden. Dennoch können Sie entfernten Clients Zugriff auf Ihr lokales Netzwerk geben. Dafür müssen Sie *Getrennte Netzwerke* festlegen, auf die vom entfernten Netzwerk aus zugegriffen werden darf. Darüber hinaus können Sie eine oder mehrere *Getrennte Domänen* festlegen, auf die zugegriffen werden darf.Falls Ihre lokalen Domänen nicht öffentlich auflösbar sind, müssen Sie einen *Getrennten DNS-Server* angeben, der Anfragen von den entfernten Clients entgegennimmt.

  Hinweis – VLAN-getaggte Datenframes können mit diesem Betriebsmodus nicht bearbeitet werden. Wenn Sie hinter Ihrer RED-Appliance ein VLAN verwenden, arbeiten Sie stattdessen im *Standard*-Modus.

Beispiele zu diesen Betriebsmodi finden Sie auf der Registerkarte *Einrichtungshilfe*.

3. **Nehmen Sie für RED 50 optional folgende Switch-Port-Konfigurationseinstellungen vor:**
   LAN-Port-Modus: RED 50 bietet vier LAN-Ports, die entweder als einfache Switches oder für eine intelligente VLAN-Nutzung konfiguriert werden können. Wenn *Switch* konfiguriert ist, wird sämtlicher Verkehr im Prinzip an alle Ports gesendet. Wenn *VLAN* konfiguriert ist, kann Verkehr gemäß den VLAN-Tags der Ethernet-Frames gefiltert werden. Dadurch kann mehr als ein Netzwerk durch den RED-Tunnel geführt werden.

   LAN-Modi: Wenn Sie Ports als VLAN-Switches konfigurieren, können Sie jeden LAN-Port separat konfigurieren. Für jeden LAN-Port sind die folgenden Optionen verfügbar:

   Ohne Tags: Ethernet-Frames mit den im Feld *LAN VID(s)* unten angegebenen VLAN-IDs werden an diesen Port gesendet. Die Frames werden ohne Tags gesendet. Daher müssen die Endgeräte VLAN nicht unbedingt unterstützen. Für diesen Port ist nur eine einzige VLAN-ID zulässig.

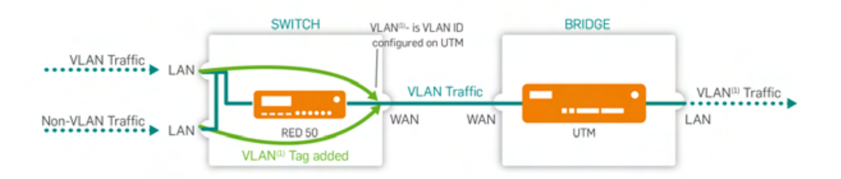


Bild 25 LAN Modus: Ohne Tags

Ohne Tags, mit Tags verwerfen: Ethernet-Frames mit den im Feld *LAN VID(s)* unten angegebenen VLAN-IDs werden nicht an diesen Port gesendet. Die Frames werden ohne Tags gesendet. Daher müssen die Endgeräte VLAN nicht unbedingt unterstützen.

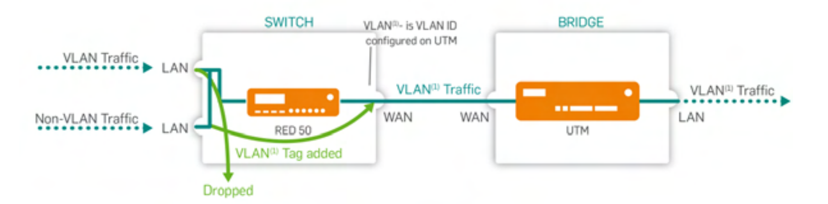


Bild 26 LAN Modus: Ohne Tags, mit Tags verwerfen

Mit Tags: Ethernet-Frames mit den im Feld *LAN VID(s)* unten angegebenen VLAN-IDs werden an diesen Port gesendet. Die Frames werden mit Tags gesendet. Daher müssen die Endgeräte VLAN unterstützen. Frames ohne VLAN-IDs werden nicht an diesen Port gesendet. Für diesen Port sind bis zu 64 verschiedene, durch Komma getrennte VLAN-IDs zulässig.

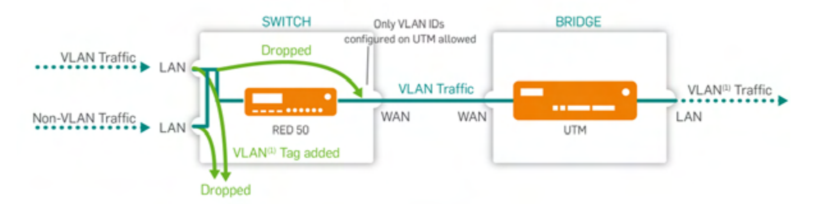


Bild 27 LAN Modus: mit Tags

Nicht verwendet: Dieser Port ist geschlossen.Keine Frames mit den oder ohne die im Feld *LAN VID(s)* angegebenen VLAN-IDs werden an diesen Port gesendet.

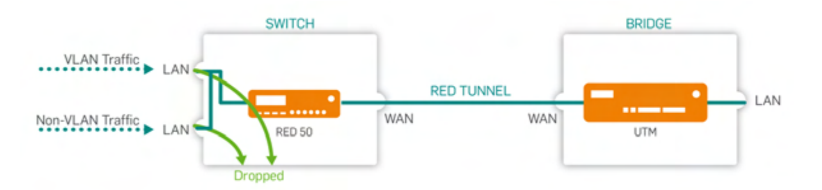


Bild 28 LAN Modus: nicht verwendet

Hinweis – Die *LAN-Modi* werden in der Cisco/HP-Dokumentation anders genannt. *Ohne Tags* wird "Hybrid-Port" genannt, *ohne Tags, mit Tags verwerfen* wird "Access-Port" genannt, *mit Tags* wird "Trunk Port" genannt.

4. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**

MAC-Filter-Typ: Um die MAC-Adressen einzuschränken, die sich mit dieser RED-Appliance verbinden dürfen, wählen Sie *Blacklist* oder *Whitelist*.Mit *Blacklist* sind alle MAC-Adressen erlaubt, außer denen, die auf der unten ausgewählten MAC-Adressliste stehen. Mit *Whitelist* sind alle MAC-Adressen verboten, außer denen, die auf der unten ausgewählten MAC-Adressliste stehen.

MAC-Adressen: Liste der MAC-Adressen, die dazu verwendet wird, den Zugang zur RED-Appliance einzuschränken. MAC-Adresslisten können auf der Registerkarte *Definitionen & Benutzer > Netzwerkdefinitionen > MAC-Adressdefinitionen* erstellt werden. Beachten Sie, dass für RED 10 maximal 200 MAC-Adressen zulässig sind, wohingegen die Liste für RED 50 bis zu 400 MAC-Adressen enthalten kann.

Hinweis – MAC-Filterung wird nur für RED Rev. 2 oder neuer unterstützt.

RED einrichten: Wählen Sie aus, wie Sie die nötigen Konfigurationseinstellungen für das RED vornehmen möchten.Standardmäßig stellt die UTM die Konfigurationsdaten des RED automatisch über den RED Provisioning Service der Sophos zur Verfügung. In diesem Fall erhält das RED seine Konfiguration über das Internet. Wenn Ihr

RED beispielsweise über keine Internetverbindung verfügt, können Sie die Konfiguration manuell, über USB-Stick, vornehmen.

Hinweis – Die manuelle Einrichtung funktioniert nur bei RED-Appliances mit Firmware-Version 9.1 oder höher.

Warnung – Wenn Sie die manuelle Einrichtung wählen, ist es extrem wichtig, den Entsperrcode aufzubewahren, der per E-Mail zugesendet wird.Wenn Sie den Entsperrcode verlieren, können Sie die RED-Appliance nie mehr mit einer anderen UTM verbinden.

Datenkomprimierung: Wenn die Datenkomprimierung aktiviert ist, wird sämtlicher Datenverkehr, der durch den RED-Tunnel geleitet wird, komprimiert. Durch die Datenkomprimierung kann sich der Durchsatz durch die RED-Appliance in Bereichen mit sehr langsamer Internetverbindung wie 1–2 Mbit/s erhöhen. Leistungsverbesserungen hängen jedoch hauptsächlich von der Entropie der gesendeten Daten ab (z. B. können bereits komprimierte Daten wie HTTPS oder SSH nicht noch weiter komprimiert werden). Unter gewissen Umständen ist es daher möglich, dass sich bei der Aktivierung der Datenkomprimierung der Durchsatz durch die RED-Appliance tatsächlich reduziert. Deaktivieren Sie in einem solchen Fall die Datenkomprimierung.

Hinweis – Datenkomprimierung ist für RED 10 Rev.1 nicht verfügbar.

3G/UMTS-Failover: Seit RED Rev. 2 besitzt die RED-Appliance einen USB-Port, in den Sie einen 3G/UMTS-USB-Stick stecken können. Wenn diese Option ausgewählt ist, kann dieser Stick bei einem Ausfall der WAN-Schnittstelle als Internet-Uplink-Failover verwendet werden. Die nötigen Einstellungen entnehmen Sie bitte dem Datenblatt Ihres Internetproviders.

- **Benutzername/Kennwort** (optional): Geben Sie, sofern erforderlich, einen Benutzernamen und ein Kennwort für das Mobilfunknetz ein.
- **PIN** (optional): Geben Sie die PIN der SIM-Karte ein, falls eine PIN konfiguriert ist.

  Hinweis – Wenn Sie eine falsche PIN eingeben, kann bei einem Ausfall der WAN-Schnittstelle die Verbindung über 3G/UMTS nicht aufgebaut

> werden.Stattdessen wird das Auswahlkästchen *3G/UMTS-Failover* der RED-Appliance automatisch deselektiert. Auf diese Weise wird die falsche PIN nur einmal verwendet. Wenn die WAN-Schnittstelle wieder funktioniert, wird für die RED-Appliance eine Warnung angezeigt: *Eine falsche PIN wurde für den 3G/UMTS-Failover-Uplink eingegeben.Bitte ändern Sie die Zugangsdaten.*Wenn Sie das Dialogfeld *RED bearbeiten* öffnen, wird eine Meldung angezeigt, die Ihnen mitteilt, dass die Auswahl von *3G/UMTS-Failover* automatisch aufgehoben wurde. Korrigieren Sie die PIN, bevor Sie die Option wieder aktivieren. Beachten Sie bitte, dass nach drei Verbindungsversuchen mit einer falschen PIN die SIM-Karte gesperrt wird.Das Entsperren der SIM-Karte ist über die RED-Appliance oder die UTM nicht möglich. Die Signalstärke für die meisten unterstützen *3G/UMTS*-USB-Sticks wird im Live-Protokoll und auf der LCD-Anzeige des RED 50 angezeigt.

- **Mobilfunknetz:** Wählen Sie den Typ des Mobilfunknetzes aus (entweder GSM oder CDMA).
- **APN:** Geben Sie den Access-Point-Name Ihres Providers ein.
- **Einwahlkennung** (optional): Sollte Ihr Dienstanbieter eine spezifische Einwahlkennung verwenden, müssen Sie diese hier eingeben. Der Standard ist *99#.

> **Hinweis –** Die folgenden Konfigurationen müssen Sie immer manuell vornehmen: 1) Das Anlegen der notwendigen Firewall-Regeln (*Network Protection* > *Firewall* > *Regeln*).2) Das Anlegen der notwendigen Maskierungsregeln (*Network Protection* > *NAT* > *Maskierung*).

5. **Klicken Sie auf *Speichern*.**
   Die RED-Appliance wird angelegt und in der Liste *RED* angezeigt.

Mit der automatischen RED-Einrichtung ruft das RED direkt nach dem Booten seine Konfiguration vom SophosRED Provisioning Service (RPS) ab. Danach wird die Verbindung zwischen Ihrer UTM und der RED-Appliance aufgebaut.

Wenn Sie die manuelle RED-Einrichtung nutzen, besitzt der neue Eintrag in der Liste *RED* eine *Download*-Schaltfläche. Laden Sie die Konfigurationsdatei herunter und speichern Sie sie im Wurzelverzeichnis eines USB-Sticks. Stecken Sie den USB-Stick dann in die RED-Appliance,

bevor Sie sie einschalten. Das RED ruft seine Konfiguration vom USB-Stick ab. Danach wird die Verbindung zwischen Ihrer UTM und der RED-Appliance aufgebaut.

Warnung – Es ist äußerst wichtig, dass Sie sich den Entsperrcode aufschreiben, der, nachdem die RED-Appliance ihre Konfiguration erhalten hat, sofort an die E-Mail-Adresse gesendet wird, die auf der Registerkarte *Allgemeine Einstellungen* angegeben ist.(Falls Sie zwischen manueller und automatischer RED-Einrichtung wechseln, müssen Sie sicherstellen, dass Sie sich beide Entsperrcodes merken.) Sie benötigen den Entsperrcode, wenn Sie die RED-Appliance mit einer anderen UTM verwenden wollen. Wenn Sie dann den Entsperrcode nicht parat haben, ist der einzige Weg, die RED-Appliance zu entsperren, den Sophos-Support zu kontaktieren. Der Support kann Ihnen jedoch nur dann helfen, wenn Sie die automatische RED-Einrichtung über den Sophos-RED-Provisioning-Service verwendet haben.

Um eine RED-Appliance zu bearbeiten, klicken Sie auf die entsprechende Schaltfläche.Sie können den Gerätestatus aller konfigurierten RED-Appliances auf der *RED*-Übersichtsseite des WebAdmin verfolgen.

Die folgenden Abbildungen geben einen Überblick über die vier möglichen Kombinationen von Lastverteilung und Failover, die RED 50 bietet. Durchgezogene Linien repräsentieren Lastverteilung, gepunktete Linien Failover-Verhalten:

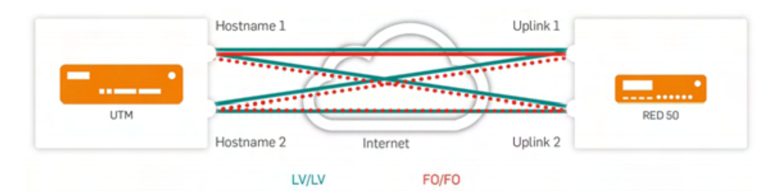


Bild 29 RED 50: Hostnamen- und Uplink-Lastverteilung (türkis) und Hostnamen- und Uplink-Failover (rot)

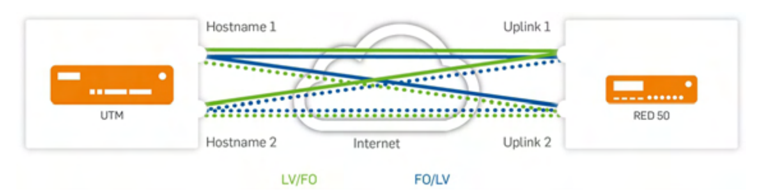


Bild 30 RED 50: Hostnamen-Lastverteilung und Uplink-Failover (grün) sowie Hostnamen-Failover und Uplink-Lastverteilung (blau)

Löschen einer RED-Appliance

Um eine RED-Appliance zu löschen, klicken Sie auf die Schaltfläche *Löschen* neben dem Namen der Appliance.
Sie werden einen Warnhinweis sehen, dass das RED-Objekt Abhängigkeiten hat. Beachten Sie, dass beim Löschen einer RED-Appliance dazugehörige Schnittstellen und deren Abhängigkeiten *nicht* gelöscht werden. Dieses Verhalten ist bewusst so gewählt, da es Ihnen ermöglicht, eine Schnittstelle von einem RED-Gerät zu einem anderen zu verschieben.

Wenn Sie eine RED-Konfiguration vollständig entfernen wollen, müssen Sie eventuelle Schnittstellen und andere Definitionen manuell löschen.

14.4 Einrichtungshilfe

Die Registerkarte *RED-Verwaltung* > *Einrichtungshilfe* verfügt über einen Assistenten, der das Einrichten und die Integration einer RED-Umgebung erleichtert. Der Assistent ist als einfache Alternative zur normalen Konfiguration auf der Registerkarte *Clientverwaltung* gedacht. Sie müssen lediglich die erforderlichen Felder ausfüllen, falls notwendig auch Felder, die als *optional* gekennzeichnet sind, und dann auf die Schaltfläche *RED einrichten* klicken.

Die Markierung *[Server]* vor dem Seitennamen gibt an, dass diese Seite nur konfiguriert werden muss, wenn die UTM als Server (RED-Hub) fungieren soll.

Hinweis – Der Einfachheit halber erstellt die Einrichtungshilfe in den Modi *Standard* und *Standard/Getrennt* im Gegensatz zur Registerkarte *Clientverwaltung* folgende Objekte automatisch: eine lokale Schnittstelle mit der festgelegten IP-Adresse; einen DHCP-Server für das entfernte Netzwerk, der die Hälfte des verfügbaren IP-Adressbereichs abdeckt; Zugriff auf die lokale DNS-Auflösung.Für den Modus *Transparent/Getrennt* legt die Einrichtungshilfe nur eine DHCP-Client-Schnittstelle an (*Ethernet-DHCP*).

Die Einrichtungshilfe bietet eine Kurzbeschreibung zu jeder Option und eine schematische Darstellung für jeden der drei Betriebsmodi, die mit der RED-Technologie möglich sind.

Unten finden Sie eine Beschreibung und Anwendungsfälle für die drei Betriebsmodi von RED.

Standard/Vereint

Die UTM verwaltet das gesamte entfernte Netzwerk.Sie fungiert als DHCP-Server und als Standardgateway.

Beispiel: Sie haben eine Zweigstelle und möchten aus Sicherheitsgründen, dass sämtlicher Verkehr der Zweigstelle über die im Hauptsitz befindliche UTM geleitet wird. Auf diese Weise wird die Zweigstelle Teil Ihres lokalen Netzwerks, als ob Sie über LAN verbunden wäre.

Standard/Getrennt

Hinweis – VLAN-getaggte Datenframes können mit diesem Betriebsmodus nicht bearbeitet werden. Wenn Sie hinter Ihrer RED-Appliance ein VLAN verwenden, arbeiten Sie stattdessen im *Standard*-Modus.

Wie im Modus *Standard* verwaltet die UTM das gesamte entfernte Netzwerk. Sie fungiert als DHCP-Server und als Standardgateway. Der Unterschied besteht darin, dass nur Netzwerkverkehr, der an Netzwerke gerichtet ist, die im Feld *Getrennte Netzwerke* aufgeführt sind, zu Ihrer lokalen UTM umgeleitet wird. Verkehr, der nicht an die definierten getrennten Netzwerke gerichtet ist, wird direkt ins Internet geroutet.

Beispiel: Sie haben eine Zweigstelle und möchten für sie Zugriff auf Ihr lokales Intranet einrichten oder den Datenverkehr des entfernten Netzwerks aus Sicherheitsgründen über Ihre UTM leiten, z. B. um die Daten auf Viren zu überprüfen oder um einen HTTP-Proxy einzusetzen.

Transparent/Getrennt

Hinweis – VLAN-getaggte Datenframes können mit diesem Betriebsmodus nicht bearbeitet werden. Wenn Sie hinter Ihrer RED-Appliance ein VLAN verwenden, arbeiten Sie stattdessen im *Standard*-Modus.

Das entfernte Netzwerk bleibt unabhängig, die UTM ist Teil dieses Netzwerks, da sie eine IP-Adresse vom entfernten DHCP-Server erhält. Nur bestimmter Verkehr des entfernten Netzwerks hat Zugriff auf bestimmte Netzwerke oder lokale Domänen von Ihnen. Da UTM keine Kontrolle über das entfernte Netzwerk hat, können lokale Domänen, die nicht öffentlich

aufgelöst werden können, nicht vom entfernten Router aufgelöst werden. Zu diesem Zweck müssen Sie einen *Getrennten DNS-Server* definieren. Das ist ein lokaler DNS-Server von Ihnen, der Anfragen von den entfernten Clients entgegennimmt.

Technisch ausgedrückt besteht eine Bridge zwischen der lokalen Schnittstelle der RED-Appliance und deren Uplink-Schnittstelle zu Ihrer lokalen UTM sowie eine Bridge zum entfernten Router.(Bei RED-50-Appliances sind die LAN-Ports nur mit WAN 1 gebridgt.) Da die UTM nur ein Client des entfernten Netzwerks ist, ist es nicht möglich, die getrennten Netzwerke auf die gleiche Weise zu routen wie in den anderen Modi. Daher liest das RED-Gerät allen Verkehr mit: Verkehr, der für ein Netzwerk bestimmt ist, das im Feld *Getrennte Netzwerke* aufgeführt ist, oder zu einer Domäne geleitet wird, die im Feld *Getrennte Domänen* aufgeführt ist, wird zur Schnittstelle der UTM umgeleitet. Dies wird erreicht, indem die MAC-Adresse des Standardgateways in den betreffenden Datenpaketen durch die MAC-Adresse von UTM ersetzt wird.

Beispiel: Sie haben einen Partner oder einen Dienstleister, der Zugang zu Ihrem Intranet oder einem bestimmten Server in Ihrem lokalen Netzwerk haben soll. Durch die Verwendung eines RED-Geräts bleibt das Netzwerk Ihres Partners vollständig unabhängig von Ihrem Netzwerk, aber er kann auf einen festgelegten Teil Ihres Netzwerks zu bestimmten Zwecken zugreifen, so als wäre er über LAN verbunden.

Hinweis – Bei Verwendung der Einrichtungshilfe ist der Uplink-Modus der RED-Appliance in jedem Betriebsmodus *DHCP-Client*. Wenn es notwendig ist, stattdessen eine statische IP-Adresse zu benutzen, müssen Sie die RED-Appliance über die Registerkarte *Clientverwaltung* konfigurieren.

14.5 Tunnelverwaltung

Auf der Seite *RED-Verwaltung* > *Tunnelverwaltung* können Sie Ihre UTM so konfigurieren, dass sie sich wie eine RED-Appliance verhält, um so einen RED-Tunnel zu einer anderen UTM aufbauen zu können. Die entfernte Host-UTM dient dann als RED-Hub für Ihre UTM.

Die Markierung *[Client]* vor dem Seitennamen gibt an, dass diese Seite nur konfiguriert werden muss, wenn die UTM als RED-Client fungieren soll.

Um Ihre UTM mit der Host-UTM zu verbinden, benötigen Sie eine Bereitstellungsdatei. Diese Datei muss auf der Host-UTM generiert werden (siehe *Clientverwaltung*).

Um Ihre UTM mit der Host-UTM zu verbinden, gehen Sie folgendermaßen vor:

1. **Fügen Sie auf der Host-UTM Ihre lokale UTM zur Liste *Clientverwaltung* hinzu.**
2. **Laden Sie auf der Host-UTM die Bereitstellungsdatei für Ihre UTM herunter.**
3. **Klicken Sie auf Ihrer lokalen UTM auf *Tunnel hinzufügen*.**
   Das Dialogfeld *Tunnel hinzufügen* wird geöffnet.
4. **Nehmen Sie die folgenden Einstellungen vor:**
   Tunnelname: Geben Sie einen aussagekräftigen Namen für diesen Tunnel ein.

   UTM-Host: Wählen Sie den entfernten UTM-Host.

   Prov.- Datei: Klicken Sie auf das Ordnersymbol, wählen Sie die Bereitstellungsdatei aus, die Sie hochladen wollen, und klicken Sie auf *Hochladen starten*.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.
5. **Klicken Sie auf *Speichern*.**
   Der RED-Tunnel wird aufgebaut und in der Liste *Tunnelverwaltung* angezeigt.

15 Site-to-Site-VPN

In diesem Kapitel wird die Konfiguration der Site-to-Site-VPN-Einstellungen von Sophos UTM beschrieben. Site-to-Site-VPNs werden in Sophos UTM über sogenannte *Virtual Private Networks* (VPNs, dt. virtuelle private Netzwerke) realisiert. Diese sind ein kostengünstiger und sicherer Weg für räumlich getrennte Netzwerke, um miteinander über ein öffentliches Netzwerk wie das Internet vertraulich zu kommunizieren. Sie verwenden das kryptografische Tunnelprotokoll IPsec, um Vertraulichkeit und Datenschutz für die übertragenen Daten zu gewährleisten.

Querverweis – Weitere Informationen zur Konfiguration von Site-to-Site-VPN-Verbindungen finden Sie in der Sophos-Knowledgebase.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Amazon VPC
- IPsec
- SSL
- Zertifikatverwaltung

Die *Site-to-Site-VPN*-Übersichtsseite im WebAdmin zeigt alle konfigurierten Amazon-VPC-, IPsec- und SSL-Verbindungen sowie deren augenblicklichen Zustand. Der Zustand einer Verbindung wird durch die Farbe ihrer Statusampel wiedergegeben. Es gibt zwei Arten von Statusampeln. Die größeren neben dem Verbindungsnamen informieren Sie über den Gesamtzustand einer Verbindung. Die verschiedenen Farben bedeuten Folgendes:

- Grün – Alle SAs (*Security Association*, dt. Sicherheitsverbindung) wurden hergestellt. Die Verbindung ist voll funktionsfähig.
- Gelb – Nicht alle SAs wurden hergestellt. Die Verbindung ist nur eingeschränkt funktionsfähig.
- Rot – Keine SAs wurden hergestellt. Die Verbindung ist nicht funktionsfähig.

Die kleineren Statusampeln neben der Information zum Tunnel geben den Zustand des Tunnels wieder. Hier bedeuten die Farben Folgendes:

- Grün – Alle SAs wurden hergestellt. Der Tunnel ist voll funktionsfähig.
- Gelb – Die IPsec-SA wurde hergestellt, die ISAKMP-SA (*Internet Security Association and Key Management Protocol*) hingegen wurde nicht hergestellt. Der Tunnel ist voll funktionsfähig.
- Rot – Keine SAs wurden hergestellt. Die Verbindung ist nicht funktionsfähig.

15.1 Amazon VPC

Die Amazon Virtual Private Cloud (VPC) ist ein kommerzieller Cloud-Computing-Dienst. Ein Benutzer kann virtuelle private Clouds anlegen, welche danach mit einem lokalen Netzwerk verbunden und zentral über IPsec-Tunnel verwaltet werden können.

Sie können Ihre Amazon VPC mit Ihrer Sophos UTM verbinden, falls die UTM eine statische öffentliche IP-Adresse besitzt. Die gesamte Konfiguration der VPN-Verbindungen muss in der Amazon-Umgebung durchgeführt werden. Danach können Sie die Verbindungsdaten einfach mit Hilfe Ihrer Amazon-Zugangsdaten oder einer Konfigurationsdatei importieren.

15.1.1 Status

Auf der Seite *Site-to-Site-VPN > Amazon VPC > Status* wird eine Liste mit allen Verbindungen zu Ihren Amazon VPCs angezeigt.

Hier können Sie die Verbindungen aktivieren und deaktivieren.

Um Verbindungen zur Amazon VPC zu aktivieren, gehen Sie folgendermaßen vor:

1. **Wählen Sie auf der Seite *Einrichtung* mindestens eine VPC-Verbindung.**
2. **Aktivieren Sie Amazon VPC auf der Seite *Status*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und die importierten VPC-Verbindungen werden angezeigt.
3. **Aktivieren Sie die gewünschte Verbindung.**
   Klicken Sie auf den Schieberegler der Verbindung, die Sie aktivieren wollen.

   Der Schieberegler wird grün und die beiden Tunnel der VPC-Verbindung werden angezeigt.

> **Hinweis –** Aus Redundanzgründen besteht jede Verbindung aus zwei Tunneln: einem aktiven und einem Ersatztunnel (Backup). Aktive Tunnel können anhand des Vorhandenseins einer Netzmaske am Ende Ihrer BGP-Zeile erkannt werden. Die Statusampeln der Tunnel werden lediglich zur Überwachung der Tunnel angezeigt – Sie können Tunnel darüber nicht aktivieren oder deaktivieren.

Um alle Amazon-VPC-Verbindungen zu deaktivieren, klicken Sie auf den obersten Schieberegler. Um eine einzelne Verbindung zu deaktivieren, klicken Sie auf den Schieberegler der jeweiligen Verbindung.

Um eine Verbindung zu schließen oder aus der Liste zu löschen, klicken Sie auf das rote Löschen-Symbol der jeweiligen Verbindung.

> **Hinweis –** Da die Verbindungen auf der Amazon-VPC-Seite konfiguriert werden, können Sie eine gelöschte Verbindung in Sophos UTM mit den ursprünglichen Daten neu importieren.

15.1.2 Einrichtung

Auf der Seite *Site-to-Site-VPN > Amazon VPC > Einrichtung* können Sie Verbindungen zu Ihrer Amazon Virtual Private Cloud (VPC) hinzufügen. Sie können entweder alle Verbindungen importieren, die gemeinsam in einem Amazon-Web-Service-(AWS)-Konto konfiguriert wurden und die IP-Adresse Ihrer Sophos UTM als *Customer Gateway* (Amazon-Ausdruck für Ihren Endpoint einer VPC-VPN-Verbindung) verwenden. Oder Sie können Verbindungen nacheinander hinzufügen, indem Sie die Konfigurationsdatei verwenden, die Sie von Amazon herunterladen können.

Import über Amazon-Zugangsdaten

Sie können alle Verbindungen auf einmal importieren, die mit einem einzigen AWS-Konto konfiguriert wurden und die IP-Adresse Ihrer Sophos UTM als Customer Gateway verwenden. Geben Sie einfach die AWS-Zugangsdaten ein, die Sie erhalten haben, als Sie Ihr Amazon-Web-Service-Konto eingerichtet haben.

> **Hinweis –** Alle vorhandenen Verbindungen, die auf der Registerkarte *Status* aufgeführt sind, werden während des Imports gelöscht.

Um Verbindungen zu importieren, gehen Sie folgendermaßen vor:

1. **Nehmen Sie die folgenden Einstellungen vor:**
   Access Key: Geben Sie Ihren Amazon Access Key ein. Dabei handelt es sich um eine Folge von 20 alphanumerischen Zeichen.

   Secret Key: Geben Sie Ihren Secret Key ein. Dabei handelt es sich um eine Folge von 40 Zeichen.

2. **Klicken Sie auf *Übernehmen*.**

   Die Verbindungen werden importiert und danach auf der Seite *Status* angezeigt.

Import über Amazon-VPC-Konfiguration

Um eine einzelne Verbindung zu einer vorhandenen Liste an Verbindungen hinzuzufügen, müssen Sie die Konfigurationsdatei der entsprechenden Verbindung hochladen.

Um eine einzelne Verbindung zu importieren, gehen Sie folgendermaßen vor:

1. **Laden Sie die Konfigurationsdatei Ihrer Amazon-VPC-Verbindung herunter.**
   Stellen Sie im Download-Dialogfenster von Amazon sicher, dass Sie *Sophos* aus der Auswahlliste *Vendor* auswählen.

2. **Öffnen Sie das Dialogfenster *Datei hochladen*.**
   Klicken Sie auf das Ordnersymbol neben dem Feld *VPC-Konfigdatei*.

3. **Wählen Sie die Konfigurationsdatei aus und laden Sie sie hoch.**
   Um die gewählte Datei hochzuladen, klicken Sie auf die Schaltfläche *Hochladen starten*.

   Der Dateiname wird im Feld *VPC-Konfigdatei* angezeigt.

4. **Wenn Sie statisches Routing verwenden, geben Sie das entfernte Netzwerk ein.**
   Das entfernte Netzwerk ist nicht Bestandteil der Konfigurationsdatei. Daher müssen Sie es getrennt in das Feld *Entferntes Netzwerk* eingeben, z. B. 10.0.0.0/8. Dieses Feld ist nur dann wichtig, wenn Sie in Amazon VPC festgelegt haben, dass statisches Routing statt dynamischen Routings verwendet wird.

5. **Klicken Sie auf *Übernehmen*.**
   Die Verbindung wird importiert und danach auf der Seite *Status* angezeigt.

Routenübertragung

Sie können Netzwerke konfigurieren, die in Routing-Tabellen in Amazon VPC übertragen werden, für die Routenübertragung aktiviert ist.

Wählen Sie lokale Netzwerke folgendermaßen aus:

1. **Fügen Sie lokale Netzwerke hinzu.**
   Fügen Sie ein lokales Netzwerk hinzu, auf das die Routenübertragung angewendet werden soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

2. **Klicken Sie auf *Übernehmen*.**
   Die Netzwerke für die Routenübertragung werden übernommen.

15.2 IPsec

IP Security (IPsec) ist ein Standard für die Sicherung von *Internet-Protocol-*(IP-)Kommunikationen durch Verschlüsselung und/oder Authentifizierung aller IP-Pakete.

Der IPsec-Standard kennt zwei Betriebsarten (Modi) und zwei Protokolle:

- Transportmodus (engl. Transport Mode)
- Tunnelmodus (engl. Tunnel Mode)
- *Authentication Header* (AH): Protokoll für Authentifizierung
- *Encapsulated Security Payload* (ESP): Protokoll für Verschlüsselung (und Authentifizierung)

Des Weiteren bietet IPsec Methoden für die manuelle und die automatische Verwaltung von *Sicherheitsverbindungen* (SAs, engl. Security Associations) sowie zur Schlüsselverteilung. Alle diese Merkmale wurden in einer *Domain of Interpretation* (DOI) zusammengefasst.

IPsec-Modi

IPsec kann entweder im Transportmodus oder im Tunnelmodus arbeiten. Eine Host-zu-Host-Verbindung kann grundsätzlich jeden Modus verwenden. Wenn es sich bei einem der beiden Tunnelendpunkte jedoch um eine Firewall handelt, muss der Tunnelmodus verwendet werden. Die IPsec-VPN-Verbindungen auf der UTM arbeiten immer im Tunnelmodus.

Im Transportmodus wird das zu bearbeitende IP-Paket nicht in ein anderes IP-Paket eingepackt. Der ursprüngliche IP-Header wird beibehalten und das übrige Paket wird entweder in Klartext (AH) oder verschlüsselt (ESP) gesendet. Nun kann entweder das komplette Paket mit AH authentifiziert oder die Payload mit Hilfe von ESP verschlüsselt und authentifiziert werden. In beiden Fällen wird der Original-Header in Klartext über das WAN geschickt.

Im Tunnelmodus wird das komplette Paket – Header und Payload – in ein neues IP-Paket gekapselt. Ein IP-Header wird vorne an das IP-Paket angehängt, wobei die Zieladresse auf den empfangenden Tunnelendpunkt gesetzt wird. Die IP-Adressen des gekapselten Paketes bleiben unverändert. Das Originalpaket kann dann mit AH authentifiziert oder mit ESP authentifiziert und verschlüsselt werden.

IPsec-Protokolle

IPsec verwendet für die sichere Kommunikation auf IP-Ebene zwei Protokolle:

- **Authentication Header (AH):** Ein Protokoll für die Authentifizierung von Absendern eines Pakets sowie zur Überprüfung der Integrität des Paketinhalts.
- **Encapsulating Security Payload (ESP):** Ein Protokoll für die Verschlüsselung des gesamten Pakets sowie für die Authentifizierung seines Inhalts.

Das *Authentication-Header*-Protokoll (AH) überprüft die Authentizität und die Integrität des Paketinhalts. Des Weiteren überprüft es, ob die Sender- und Empfänger-IP-Adressen während der Übertragung geändert wurden. Die Authentifizierung des Pakets erfolgt anhand einer Prüfsumme, die mittels eines *Hash-based Message Authentication Codes* (HMAC) in Verbindung mit einem Schlüssel und einem Hash-Algorithmus berechnet wurde. Einer der folgenden Hash-Algorithmen wird verwendet:

- **Message Digest Version 5 (MD5):** Dieser Algorithmus erzeugt aus einer Nachricht mit beliebiger Länge eine 128-Bit-lange Prüfsumme. Diese Prüfsumme ist wie ein Fingerabdruck des Paketinhalts und ändert sich, wenn die Nachricht verändert wird. Dieser Hash-Wert wird manchmal auch als digitale Signatur oder als Message Digest bezeichnet.
- **Secure Hash (SHA-1):** Dieser Algorithmus erzeugt analog zum MD5 einen 160-Bit-langen Hash-Wert. SHA-1 ist aufgrund des längeren Schlüssels sicherer als MD5.

Der Aufwand, einen Hash-Wert mittels SHA-1 zu berechnen, ist im Vergleich zum MD5-Algorithmus etwas höher. Die Berechnungsgeschwindigkeit hängt natürlich von der Prozessorgeschwindigkeit und der Anzahl der IPsec-VPN-Verbindungen ab, die auf der Sophos UTM verwendet werden.

Das *Encapsulated-Security-Payload*-Protokoll (ESP) bietet zusätzlich zur Verschlüsselung auch die Möglichkeit, den Absender zu authentifizieren und den Paketinhalt zu verifizieren. Wenn ESP im Tunnelmodus verwendet wird, wird das komplette IP-Paket (Header und Payload) verschlüsselt. Zu diesem verschlüsselten Paket wird ein neuer unverschlüsselter IP- und ESP-Header hinzugefügt: Der neue IP-Header beinhaltet die Adresse des Empfänger-

Gateways und die Adresse des Absender-Gateways. Diese IP-Adressen entsprechen denen des VPN-Tunnels.

Für ESP mit Verschlüsselung werden üblicherweise die folgenden Algorithmen verwendet:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Von diesen bietet AES den höchsten Sicherheitsstandard. Die effektiven Schlüssellängen, die mit AES verwendet werden können, sind 128, 192 oder 256 Bit. Sophos UTM unterstützt mehrere Verschlüsselungs-Algorithmen. Für die Authentifizierung kann der MD5- oder der SHA-1-Algorithmus verwendet werden.

NAT-Traversal (NAT-T)

NAT-Traversal ist ein Verfahren, um zwischen Hosts in TCP/IP-Netzwerken Verbindungen über NAT-Geräte aufzubauen. Dies wird erreicht, indem UDP-Verkapselung der ESP-Pakete genutzt wird, um IPsec-Tunnel über NAT-Geräte aufzubauen. Die UDP-Verkapselung wird nur verwendet, wenn zwischen den IPsec-Gegenstellen NAT gefunden wird; andernfalls werden normale ESP-Pakete verwendet.

Mit NAT-Traversal kann ein IPsec-Tunnel auch aufgebaut werden, wenn sich das Gateway oder ein Road Warrior hinter einem NAT-Router befindet. Wenn Sie diese Funktion nutzen wollen, müssen allerdings beide IPsec-Endpunkte NAT-Traversal unterstützen – das wird automatisch ausgehandelt. Zusätzlich muss auf dem NAT-Gerät der IPsec-Passthrough (IPsec-Durchreichung) ausgeschaltet sein, da dies NAT-Traversal beeinträchtigen kann.

Wenn Road Warriors NAT-Traversal verwenden wollen, muss ihr entsprechendes Benutzerobjekt im WebAdmin eine statische Fernzugriffs-IP-Adresse (RAS, engl. remote static IP address) besitzen (siehe auch *Statische Fernzugriffs-IP verwenden* auf der Seite *Benutzer* im WebAdmin).

Um zu verhindern, dass der Tunnel abgebaut wird, wenn keine Daten übermittelt werden, sendet NAT-Traversal standardmäßig in einem Intervall von 60 Sekunden ein Signal zur Aufrechterhaltung (engl. keep alive).Durch dieses Aufrechterhaltungssignal wird sichergestellt, dass der NAT-Router die Statusinformation der Sitzung behält, damit der Tunnel offen bleibt.

TOS

Type-of-Service-Bits (TOS) sind einige Vier-Bit-Flags im IP-Header. Die Bits werden *Type-of-Service*-Bits genannt, da sie es der übertragenden Anwendung ermöglichen, dem Netzwerk mitzuteilen, welche Art von Dienstqualität benötigt wird.

Bei der IPsec-Implementierung von Sophos UTM wird der TOS-Wert immer kopiert.

15.2.1 Verbindungen

Auf der Registerkarte *Site-to-Site-VPN > IPsec > Verbindungen* können Sie IPsec-Verbindungen anlegen und bearbeiten.

Um eine IPsec-Verbindung zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue IPsec-Verbindung*.**
   Das Dialogfeld *IPsec-Verbindung hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Verbindung ein.

   Entferntes Gateway: Wählen Sie eine Gateway-Definition für das entfernte Gateway. Entfernte Gateways werden auf der Registerkarte *Site-to-Site-VPN > IPsec > Entfernte Gateways* definiert.

   Lokale Schnittstelle: Wählen Sie den Namen der Schnittstelle aus, die als lokaler Endpoint für den IPsec-Tunnel dienen soll.

   Richtlinie: Wählen Sie die IPsec-Richtlinie für diese IPsec-Verbindung aus.IPsec-Richtlinien können auf der Registerkarte *Site-to-Site-VPN > IPsec > Richtlinien* definiert werden.

   Lokale Netzwerke: Wählen Sie die lokalen Netzwerke aus, die über den VPN-Tunnel erreichbar sein sollen, oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Automatische Firewallregeln:Wählen Sie diese Option, um automatisch Firewallregeln hinzuzufügen, die Datenverkehr für diese Verbindung zulassen. Die Regeln werden hinzugefügt, sobald die Verbindung aktiviert wird und sie werden entfernt, wenn die Verbindung deaktiviert wird. Wenn Sie eine striktere IPsec-Verbindung wünschen,

deaktivieren Sie die Option *Automatische Firewallregeln* und verwenden Sie stattdessen IPsec-Objekte im Firewallregelwerk.

Striktes Routing: Wenn diese Funktion eingeschaltet ist, erfolgt das VPN-Routing nicht nur anhand der Zieladresse, sondern anhand von Quell- und Zieladresse. Auf diese Weise werden nur Datenpakete durch den VPN-Tunnel geleitet, die mit der Tunneldefinition exakt übereinstimmen. Als Folge davon können Sie kein SNAT verwenden, um Netzwerke oder Hosts zum VPN-Tunnel hinzuzufügen, die nicht von vornherein Teil der Tunneldefinition sind. Andererseits können Sie, wenn striktes Routing ausgeschaltet ist, keine gemischte unverschlüsselte/verschlüsselte Konfiguration für dasselbe Netzwerk je nach Quelladresse haben.

Tunnel an lokale Schnittstelle binden: Standardmäßig ist diese Option deaktiviert und der gesamte Verkehr aus den gewählten lokalen Netzwerken in die festgelegten entfernten Netzwerke wird immer durch diesen IPsec-Tunnel geschickt. Mehrere identische Tunnel auf verschiedenen Schnittstellen sind nicht möglich, da sich der IPsec-Verkehr nicht unterscheiden lässt. Ist die Option jedoch aktiv, wird die hier definierte IPsec-Auswahl an die gewählte lokale Schnittstelle gebunden. Auf diese Weise ist es möglich, beispielsweise IPsec-Richtlinien mit statischen Routen zu umgehen oder redundante IPsec-Tunnel über verschiedene Uplinks zu definieren und dann den Verkehr mit Hilfe von Multipathregeln über die verfügbaren Schnittstellen und ihre IPsec-Tunnel auszugleichen. Mögliche Anwendungsfälle sind beispielsweise:

- Umgehen von IPsec-Richtlinien für lokale Hosts, die zu dem entfernten Netzwerk gehören, mit Hilfe von statischen Routen.
- Ausgleichen von Verkehr auf Layer 3 und Layer 4 mit Multipathregeln über mehrere IPsec-Tunnel oder MPLS-Links mit automatischem Failover.

Hinweis – Diese Option kann nicht zusammen mit einer Schnittstellengruppe verwendet werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Verbindung wird in der IPsec-Liste *Verbindungen* angezeigt.

Um eine Verbindung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Das IPsec-VPN-Live-Protokoll dient zur Überwachung der aufgebauten IPsec-Verbindungen. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

15.2.2 Entfernte Gateways

Auf der Registerkarte *Site-to-Site-VPN > IPsec > Entfernte Gateways* können Sie die entfernten Gateways (engl. remote gateways) für Ihre Site-to-Site-VPN-Tunnel definieren. Diese Remote-Netzwerk-Definitionen stehen dann für die Konfiguration der IPsec-Verbindungen auf der Registerkarte *IPsec > Verbindungen* zur Verfügung.

Um ein entferntes Gateway hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Entfernte Gateways* auf *Neues entferntes Gateway*.**
   Das Dialogfeld *Entferntes Gateway hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für das entfernte Gateway ein.

   Gateway-Typ: Wählen Sie den Gateway-Typ aus. Die folgenden Typen sind verfügbar:

   - **Verbindung initiieren:** Wählen Sie diesen Typ aus, wenn der entfernte Endpoint eine statische IP-Adresse besitzt, sodass das Gateway eine Verbindung zum entfernten Gateway initiieren kann. Wenn Sie diese Option gewählt haben, geben Sie im Feld *Gateway* das entfernte Gateway an. Beachten Sie, dass Sie diesen Typ auch wählen können, wenn das entfernte Gateway über DynDNS aufgelöst werden kann.

   - **Nur antworten:** Wählen Sie diesen Typ aus, wenn die IP-Adresse des entfernten Endpoints unbekannt ist oder nicht über DynDNS aufgelöst werden kann. Das Gateway ist nicht in der Lage, eine Verbindung zu dem entfernten Gateway aufzubauen und wartet deshalb auf eingehende Verbindungen, auf die es lediglich antworten muss.

   Auth.-Methode: Wählen Sie die Authentifizierungsmethode für diese Definition des entfernten Gateways aus. Die folgenden Typen sind verfügbar:

   - **Verteilter Schlüssel:** Authentifizierung mit *Verteilten Schlüsseln* (PSK, engl. Preshared Keys) verwendet geheime Kennwörter als Schlüssel. Diese Kennwörter müssen an die Endpunkte verteilt werden, bevor eine Verbindung aufgebaut wird. Wenn ein neuer VPN-Tunnel aufgebaut ist, überprüft jede Seite, ob

die andere Seite das geheime Kennwort kennt. Die Sicherheit der PSKs hängt von der Qualität der verwendeten Kennwörter ab: Normale Wörter und Ausdrücke fallen schnell Wörterbuchangriffen zum Opfer. Permanente oder längerfristige IPsec-Verbindungen sollten stattdessen Zertifikate verwenden.

- **RSA-Schlüssel:** Authentifizierung mit RSA-Schlüsseln ist technisch ausgefeilter. Bei dieser Methode erzeugt jede Seite der Verbindung ein Schlüsselpaar, das aus einem öffentlichen (engl. public key) und einem privaten Schlüssel (engl. private key) besteht. Der private Schlüssel wird zur Verschlüsselung und Authentifizierung während des Schlüsselaustauschs benötigt. Beide Endpoints einer IPsec-VPN-Verbindung benötigen bei dieser Authentifizierungsmethode ihr eigenes Schlüsselpaar.Kopieren Sie den öffentlichen RSA-Schlüssel der Gegenstelle (*Site-to-Site-VPN > IPsec > Lokaler RSA-Schlüssel*) in das Feld *Öffentlicher Schlüssel* auf dem lokalen System und andersherum. Geben Sie darüber hinaus die VPN-ID-Typen und die VPN-IDs an, die zu den entsprechenden RSA-Schlüsseln gehören.
- **Lokales X.509-Zertifikat:** Das X.509-Zertifikat basiert ähnlich wie die Authentifizierung mit RSA-Schlüsseln auf öffentlichen Schlüsseln und privaten Schlüsseln. Ein X.509-Zertifikat enthält den öffentlichen Schlüssel zusammen mit zusätzlichen Informationen über den Besitzer des Schlüssels.Solche Zertifikate sind von einer CA (*Zertifizierungsstelle*, engl. Certificate Authority) signiert und ausgestellt, der der Besitzer vertraut. Während des Schlüsselaustauschs werden die Zertifikate ausgetauscht und mit Hilfe lokal gespeicherter CA-Zertifikate authentifiziert. Wählen Sie diese Authentifizierungsmethode aus, wenn das X.509-Zertifikat des entfernten VPN-Gateways auf dem lokalen System gespeichert ist.
- **Remote-X.509-Zertifikat:** Wählen Sie diese Authentifizierungsmethode aus, wenn das X.509-Zertifikat des entfernten VPN-Gateways nicht auf dem lokalen System gespeichert ist. In diesem Fall müssen Sie den VPN-ID-Typ und die VPN-ID des Zertifikats angeben, das auf dem entfernten VPN-Gateway genutzt wird, d. h. das Zertifikat, das im Bereich *Lokales X.509-Zertifikat* auf der Registerkarte *Site-to-Site-VPN > IPsec > Erweitert* ausgewählt ist.

VPN-ID-Typ: Abhängig von der ausgewählten Authentifizierungsmethode müssen Sie einen VPN-ID-Typ und eine VPN-ID angeben. Die hier angegebene VPN-ID muss mit dem Wert auf der Gegenstelle übereinstimmen. Angenommen, Sie verwenden zwei UTM-Appliances, um einen Site-to-Site-VPN-Tunnel aufzubauen. Wenn Sie dann als Authentifizierungsmethode *RSA-Schlüssel* auf dem lokalen System auswählen, müssen

der VPN-ID-Typ und die VPN-ID mit dem übereinstimmen, was auf der Registerkarte *Site-to-Site-VPN > IPsec > Lokaler RSA-Schlüssel* der Gegenstelle konfiguriert ist.Sie können zwischen den folgenden VPN-ID-Typen wählen:

- **IP-Adresse**
- **Hostname**
- **E-Mail-Adresse**
- **Distinguished Name:** Nur bei der Authentifizierungsmethode *Remote-X.509-Zertifikat* verfügbar.
- **Any:** Standard beim Gateway-Typ *Nur antworten*.

Entfernte Netzwerke: Wählen Sie die entfernten Netzwerke aus, die über das entfernte Gateway erreichbar sein sollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Nehmen Sie gegebenenfalls erweiterte Einstellungen vor.**
Die folgenden erweiterten Einstellungen sollten Sie nur vornehmen, wenn Ihnen die Auswirkungen bekannt sind:

Pfad-MTU-Ermittlung zulassen:PMTU (Path Maximum Transmission Unit) bezeichnet die Größe der übermittelten Datenpakete. Die gesendeten IP-Datenpakete sollten so groß sein, dass sie gerade noch ohne Fragmentierung entlang der Strecke zum Ziel transportiert werden können. Zu große Datenpakete werden von den Routern auf der Strecke verworfen, wenn diese Pakete ohne Fragmentierung nicht weitergeleitet werden können. An die Absender werden dann ICMP-Pakete mit der Nachricht *ICMP Destination Unreachable* (dt. ICMP-Ziel nicht erreichbar) sowie einem Code gesendet, der „Fragmentierung benötigt und DF gesetzt" bedeutet. Aufgrund dieser Nachricht setzt der Quellhost seinen angenommenen PMTU-Wert für die Strecke herab.
Wenn Sie diese Option aktivieren, aktiviert die UTM PMTU, wenn dies auf Serverseite aktiviert ist.

Überlastkontrolle (ECN) unterstützen: ECN (Explicit Congestion Notification) ist eine Erweiterung des Internetprotokolls und ermöglicht End-to-End-Benachrichtigungen über Netzwerküberlastungen, ohne dass Pakete verworfen werden. Wählen Sie diese Option, wenn Sie ECN-Daten aus dem ursprünglichen IP-Paket-Header in den IPsec-Paket-Header kopieren möchten. Beachten Sie, dass der entfernte Endpoint

ECN ebenso unterstützen muss wie das zugrunde liegende Netzwerk und die beteiligten Router.

XAUTH-Client-Modus aktivieren: XAUTH ist eine Erweiterung von IPsec-IKE, um Benutzer über Benutzername und Kennwort auf einem VPN-Gateway zu authentifizieren. Um XAUTH für die Authentifizierung auf diesem entfernten Gateway zu verwenden, wählen Sie die Option aus und geben Sie den Benutzernamen und das Kennwort (zweimal) an, das vom entfernten Gateway erwartet wird.

4. **Klicken Sie auf *Speichern*.**
   Die Gateway-Definition wird in der Liste *Entfernte Gateways* angezeigt.

Um eine Definition eines entfernten Gateways zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

15.2.3 Richtlinien

Auf der Registerkarte *IPsec > Richtlinien* können Sie die Parameter für IPsec-Verbindungen definieren und in einer Richtlinie (Policy) zusammenfassen. Eine IPsec-Richtlinie legt die Internet-Schlüsselaustausch-Methode (IKE, Internet Key Exchange) und die IPsec-Antragsparameter für eine IPsec-Verbindung fest. Jede IPsec-Verbindung benötigt eine IPsec-Richtlinie.

Hinweis – Sophos UTM in IKE-Phase 1 wird nur der Hauptmodus unterstützt. Der aggressive Modus (engl. aggressive mode) wird nicht unterstützt.

Um eine IPsec-Richtlinie zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Richtlinie* auf *Neue IPsec-Richtlinie*.**
   Das Dialogfeld *IPsec-Richtlinie hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Richtlinie ein.

   IKE-Verschlüsselungsalgorithmus: Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der IKE-Nachrichten verwendet wird. Die folgenden Algorithmen werden unterstützt:

   - *DES* (56 Bit)
   - *3DES* (168 Bit)
   - *AES 128* (128 Bit)

- *AES 192* (192 Bit)
- *AES 256* (256 Bit)
- *Blowfish* (128 Bit)
- *Twofish* (128 Bit)
- *Serpent* (128 Bit)

Sicherheitshinweis – Es wird dringend davon abgeraten, DES zu verwenden, da dieser schwache Algorithmus eine potentielle Schwachstelle darstellt.

IKE-Authentifizierungsalgorithmus: Der Authentifizierungsalgorithmus legt fest, welcher Algorithmus verwendet wird, um die Intaktheit der IKE-Nachrichten zu prüfen. Die folgenden Algorithmen werden unterstützt:

- *MD5* (128 Bit)
- *SHA1* (160 Bit)
- *SHA2 256* (256 Bit)
- *SHA2 384* (384 Bit)
- *SHA2 512* (512 Bit)

IKE-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IKE-SA (Security Association, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 28800 Sekunden (8 Std.). Als Standardwert sind 7800 Sekunden voreingestellt.

IKE-DH-Gruppe: Während der Aushandlung einer Verbindung gleichen die beiden Gegenstellen auch die aktuellen Schlüssel für die Datenverschlüsselung ab. Für die Generierung des Sitzungsschlüssels (session key) nutzt IKE den *Diffie-Hellman*-(DH-) Algorithmus. Dieser Algorithmus generiert den Schlüssel per Zufallsprinzip basierend auf sogenannten Pool Bits. Die IKE-Gruppe gibt hauptsächlich Aufschluss über die Anzahl der Pool Bits. Je mehr Pool Bits, umso länger ist die zufällige Zahlenkette – je größer die Zahlenkette, umso schwerer kann der Diffie-Hellman-Algorithmus geknackt werden. Folglich bedeuten mehr Pool Bits höhere Sicherheit, was allerdings auch bedeutet, dass mehr CPU-Leistung für die Generierung benötigt wird. Momentan werden die folgenden Diffie-Hellman-Gruppen unterstützt:

- *Gruppe 1: MODP 768*
- *Gruppe 2: MODP 1024*
- *Gruppe 5: MODP 1536*
- *Gruppe 14: MODP 2048*
- *Gruppe 15: MODP 3072*
- *Gruppe 16: MODP 4096*

Sicherheitshinweis – Gruppe 1 (MODP 768) wird allgemein als sehr schwach eingestuft und wird hier nur aus Kompatibilitätsgründen unterstützt. Wir raten dringend davon ab, sie zu verwenden, da sie eine potenzielle Schwachstelle darstellt.

IPsec-Verschlüsselungsalgorithmus: Die gleichen Verschlüsselungsalgorithmen wie für IKE.Zusätzlich gibt es die folgenden Einträge:

- *Keine Verschlüsselung (null)*
- *AES 128 CTR* (128 Bit)
- *AES 192 CTR* (192 Bit)
- *AES 256 CTR* (256 Bit)
- *AES 128 GCM (96 Bit)*
- *AES 192 GCM (96 Bit)*
- *AES 256 GCM (96 Bit)*
- *AES 128 GCM (128 Bit)*
- *AES 192 GCM (128 Bit)*
- *AES 256 GCM (128 Bit)*

Sicherheitshinweis – Wir raten dringend davon ab, keine Verschlüsselung oder DES zu verwenden, da beides eine potenzielle Schwachstelle darstellt.

IPsec-Authentifizierungsalgorithmus: Die gleichen Authentifizierungsalgorithmen wie für IKE.Zusätzlich werden noch folgende Algorithmen unterstützt:

- *SHA2 256* (96 Bit)
- *SHA2 384* (96 Bit)
- *SHA2 512* (96 Bit)

Diese sind für die Kompatibilität mit Tunnelendpunkten verfügbar, die nicht RFC 4868 entsprechen, beispielsweise frühere UTM-Versionen (d. h. ASG-Versionen) als V8, und deshalb keine abgeschnittenen Prüfsummen länger als 96 Bit unterstützen.

IPsec-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IPsec-SA (Security Association, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 86400 Sekunden (1 Tag). Als Standardwert sind 3600 Sekunden voreingestellt.

IPsec-PFS-Gruppe: *Perfect Forward Secrecy* (PFS) ist eine Eigenschaft von Verschlüsselungsverfahren, die sicherstellt, dass aus einem geknackten Schlüssel nicht auf vorhergehende oder nachfolgende Sitzungsschlüssel einer Kommunikationsverbindung geschlossen werden kann. Damit PFS besteht, darf der zum Schutz der IPsec-SA-Verbindung genutzte Schlüssel nicht von demselben zufällig erzeugten Verschlüsselungsmaterial hergeleitet worden sein wie die Schlüssel für die IKE-SA-Verbindung. Daher initiiert PFS einen zweiten Diffie-Hellman-Schlüsselaustausch mit der Absicht, der ausgewählten DH-Gruppe für die IPsec-Verbindung einen neuen zufällig erzeugten Schlüssel zu übergeben. Es werden die gleichen DH-Gruppen wie bei IKE unterstützt.
Die Aktivierung von PFS wird als sicherer eingestuft, aber es benötigt auch mehr Zeit bei der Aushandlung. Es wird davon abgeraten, PFS auf langsamer Hardware einzusetzen.

Hinweis – PFS ist nicht immer gänzlich kompatibel mit den verschiedenen Herstellern. Wenn Sie Probleme während der Aushandlung feststellen, schalten Sie diese Funktion aus.

Strikte Richtlinie: Wenn ein IPsec-Gateway eine Anfrage hinsichtlich eines Verschlüsselungsalgorithmus und der Verschlüsselungsstärke unternimmt, kann es vorkommen, dass das Gateway des Empfängers diese Anfrage akzeptiert, obwohl das nicht mit der entsprechenden IPsec-Richtlinie übereinstimmt. Wenn Sie diese Option wählen und der entfernte Endpunkt nicht exakt die von Ihnen festgelegten Parameter verwenden will, kommt keine IPsec-Verbindung zustande. Angenommen, die IPsec-Richtlinie Ihrer UTM verlangt AES-256-Verschlüsselung, wohingegen ein Road Warrior mit

SSH-Sentinel sich mit AES-128 verbinden will – wenn die Option für die strikte Richtlinie aktiviert ist, wird die Verbindung abgewiesen.

Hinweis – Die Komprimierungseinstellung wird durch Aktivierung der Option *Strikte Richtlinie* nicht erzwungen.

Komprimierung: Diese Option legt fest, ob IP-Pakete vor der Verschlüsselung mit dem *IP Payload Compression Protocol* (IPComp) komprimiert werden. IPComp reduziert die Größe von IP-Paketen, indem es sie komprimiert, um die allgemeine Kommunikationsleistung zwischen einem Paar von kommunizierenden Hosts oder Gateways zu erhöhen. Komprimierung ist standardmäßig ausgeschaltet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Richtlinie wird in der Liste *Richtlinien* angezeigt.

Um eine Richtlinie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

15.2.4 Lokaler RSA-Schlüssel

Bei der RSA-Authentifizierung werden zur Authentifizierung der VPN-Endpoints RSA-Schlüssel verwendet. Die öffentlichen Schlüssel der Endpoints werden manuell ausgetauscht, bevor die Verbindung aufgebaut wird. Wenn Sie diese Authentifizierungsmethode verwenden möchten, müssen Sie eine VPN-ID definieren und einen lokalen RSA-Schlüssel generieren. Der öffentliche RSA-Schlüssel des Gateways muss anschließend den IPsec-Geräten der Gegenstelle zugänglich gemacht werden, die IPsec-RSA-Authentifizierung für Sophos UTM verwenden.

Aktueller lokaler öffentlicher RSA-Schlüssel

In diesem Feld wird der öffentliche Teil des aktuell installierten RSA-Schlüsselpaares angezeigt. Um den Schlüssel in die Zwischenablage zu kopieren, klicken Sie in das Feld, drücken Sie `STRG-A` und anschließend `STRG-C`.

VPN-Optionen für lokalen RSA-Schlüssel

Wählen Sie den VPN-ID-Typ entsprechend Ihren Anforderungen aus. Standardmäßig ist der Hostname des Gateways als VPN-ID voreingestellt. Wenn Sie eine statische IP-Adresse als

VPN-Endpoint haben, wählen Sie *IP-Adresse*. Verwenden Sie alternativ eine E-Mail-Adresse als VPN-ID für mobile IPsec-Road-Warriors.

- **Hostname:** Standardeinstellung; der Hostname des Gateways. Sie können jedoch auch einen anderen Hostnamen eingeben.
- **E-Mail-Adresse:** Standardmäßig ist die E-Mail-Adresse des Admin-Kontos des Gateways voreingestellt. Sie können aber eine beliebige andere E-Mail-Adresse eingeben.
- **IP-Adresse:** Die IP-Adresse der externen Schnittstelle des Gateways.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.Änderungen haben keine Auswirkungen auf den RSA-Schlüssel.

Lokalen RSA-Schlüssel neu erstellen

Um einen neuen RSA-Schlüssel zu generieren, wählen Sie die gewünschte Schlüssellänge aus und klicken Sie auf die Schaltfläche *Übernehmen*. Anschließend wird der Generierungsprozess gestartet, der – abhängig von der Schlüssellänge und der verwendeten Hardware – zwischen ein paar Minuten und zwei Stunden benötigen kann. Die Schlüssellänge ist ein Maß für die Anzahl der Schlüssel, die bei einer Chiffre möglich sind. Die Länge wird üblicherweise in Bit angegeben. Die folgenden Schlüssellängen werden unterstützt:

- 1024 Bit
- 2048 Bit
- 4096 Bit

Sobald der neue RSA-Schlüssel generiert wurde, wird der zugehörige öffentliche Schlüssel im Feld *Aktueller lokaler öffentlicher RSA-Schlüssel* angezeigt. Die Generierung eines neuen RSA-Schlüssels überschreibt den alten Schlüssel.

15.2.5 Erweitert

Auf der Registerkarte *Site-to-Site-VPN > IPsec > Erweitert* können Sie die erweiterten Einstellungen für IPsec-VPN vornehmen. Abhängig von Ihrer bevorzugten Authentifizierungsmethode können Sie unter anderem das lokale Zertifikat (für X.509-Authentifizierung) und den lokalen RSA-Schlüssel (für RSA-Authentifizierung) festlegen. Diese Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

Lokales X.509-Zertifikat

Bei der X.509-Authentifizierung werden Zertifikate verwendet, um die öffentlichen Schlüssel der VPN-Endpunkte zu überprüfen. Wenn Sie diese Authentifizierungsmethode verwenden wollen, müssen Sie im Abschnitt *Lokales X.509-Zertifikat* ein lokales Zertifikat aus der Auswahlliste wählen. Das ausgewählte Zertifikat bzw. der Schlüssel wird anschließend dafür genutzt, das Gateway gegenüber Gegenstellen zu authentifizieren, falls X.509-Authentifizierung ausgewählt ist.

Sie können nur Zertifikate auswählen, für die auch der zugehörige private Schlüssel vorhanden ist, andere Zertifikate sind in der Auswahlliste nicht verfügbar.

Wenn keine Zertifikate zur Auswahl angezeigt werden, müssen Sie zunächst eines im Menü *Zertifikatverwaltung* hinzufügen, entweder indem Sie ein neues erzeugen oder indem Sie eines über die Hochladen-Funktion importieren.

Nachdem Sie das Zertifikat ausgewählt haben, geben Sie das Kennwort ein, mit dem der private Schlüssel geschützt ist. Während des Speichervorgangs wird das Kennwort verifiziert und eine Fehlermeldung angezeigt, falls das Kennwort nicht zum verschlüsselten Schlüssel passt.

Sobald ein aktiver Schlüssel oder ein Zertifikat ausgewählt ist, wird er/es im Abschnitt *Lokales X.509-Zertifikat* angezeigt.

Dead Peer Detection (DPD)

Dead Peer Detection verwenden: Die IPsec-Verbindung wird automatisch beendet, wenn das VPN-Gateway oder der Client auf der Gegenseite nicht erreichbar ist. Bei Verbindungen mit statischen Endpunkten wird der Tunnel nach einem Ausfall automatisch neu ausgehandelt. Für Verbindungen mit dynamischen Endpunkten wird für eine neue Aushandlung des Tunnels die Anfrage seitens der Gegenstelle benötigt. In der Regel ist diese Funktion betriebssicher und kann immer eingeschaltet bleiben. Die IPsec-Partner bestimmen automatisch, ob die Gegenstelle Dead Peer Detection unterstützt oder nicht, und verwenden den normalen Modus, falls nötig.

NAT-Traversal (NAT-T)

NAT-Traversal verwenden: Wählen Sie diese Option, um zu ermöglichen, dass IPsec-Verkehr Upstream-Systeme passieren kann, die *Network Address Translation* (NAT, dt. Netzwerkadressumsetzung) verwenden. Zusätzlich können Sie das Intervall für die Aufrechterhaltung (engl. keep-alive) für NAT-Traversal festlegen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

CRL-Handhabung

Es sind Situationen denkbar, in denen ein Zertifikataussteller noch während der Gültigkeitsdauer eines Zertifikats die darin gegebene Bestätigung für ungültig erklären möchte, z. B. weil zwischenzeitlich bekannt wurde, dass das Zertifikat vom Zertifikatnehmer unter Angabe falscher Daten (Name usw.) erschlichen wurde oder weil der zum zertifizierten öffentlichen Schlüssel gehörende private Schlüssel einem Angreifer in die Hände gefallen ist. Zu diesem Zweck werden sogenannte *Zertifikatsperrlisten* (CRLs, engl. Certificate Revocation Lists) verwendet. Diese enthalten üblicherweise die Seriennummern derjenigen Zertifikate einer Zertifizierungsinstanz, die für ungültig erklärt werden und deren regulärer Gültigkeitszeitraum noch nicht abgelaufen ist.
Nach Ablauf dieses Zeitraums besitzt das Zertifikat in jedem Fall keine Gültigkeit mehr und muss daher auch nicht weiter auf der Zertifikatsperrliste geführt werden.

Automatische Abholung: Mit dieser Funktion wird die CRL automatisch über die URL abgeholt, die im Partnerzertifikat angegeben ist, via HTTP, anonymes FTP (Anonymous FTP) oder LDAP Version 3. Die CRL kann auf Anfrage heruntergeladen, abgespeichert und aktualisiert werden, sobald der Gültigkeitszeitraum abgelaufen ist. Wenn Sie diese Funktion nutzen (jedoch nicht über Port 80 oder 443), achten Sie darauf, dass die Firewallregeln so gesetzt sind, dass auf den CRL-Distributionsserver zugegriffen werden kann.

Strikte Richtlinie: Wenn Sie diese Option auswählen, werden alle Partnerzertifikate ohne eine zugehörige CRL zurückgewiesen.

Probing von verteilten Schlüsseln

Für IPsec-Verbindungen, die im Nur-Antworten-Modus (engl. respond-only) arbeiten, können Sie festlegen, dass mehrere verteilte Schlüssel (PSK, engl. preshared keys) für jede IPsec-Verbindung zugelassen sind.

Probing von verteilten Schlüsseln: Markieren Sie das Auswahlkästchen, um die Funktion zu aktivieren. Diese Option betrifft L2TP-über-IPsec-, IPsec-Fernzugriff- und IPsec-Site-to-Site-Verbindungen.

15.2.6 Fehlersuche

IKE-Fehlersuche

Im Abschnitt *IKE-Fehlersuche* können Sie die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest, für welche Arten von IKE-Nachrichten oder -Kommunikation

zusätzliche Informationen in das Fehlerprotokoll geschrieben werden.

Hinweis – Der Abschnitt *IKE-Fehlersuche* ist für die Registerkarten *Fehlersuche* der Menüs *Site-to-Site VPN IPsec*, *Fernzugriff IPsec*, *L2TP über IPsec* und *Cisco VPN Client identisch*.

Die folgenden Flags können protokolliert werden:

- **Datenflusskontrolle:** Kontrollnachrichten zum IKE-Status
- **Ausgehende Pakete:** Inhalte von ausgehenden IKE-Nachrichten
- **Eingehende Pakete:** Inhalte von eingehenden IKE-Nachrichten
- **Kernel-Messaging:** Kommunikationsnachrichten mit dem Kernel
- **Hochverfügbarkeit:** Kommunikation mit anderen Hochverfügbarkeitsknoten

15.3 SSL

Site-to-Site-VPN-Tunnel können über eine SSL-Verbindung aufgebaut werden. SSL-VPN-Verbindungen benutzen dabei eindeutige Rollen. Die Tunnelendpunkte agieren entweder als Client oder als Server. Es ist stets der Client, der die Verbindung initiiert, während der Server auf Client-Anfragen antwortet. Denken Sie daran, dass hierin der Unterschied zu IPsec liegt, wo normalerweise beide Endpunkte eine Verbindung initiieren können.

Hinweis – Wenn Sie Probleme haben, eine Verbindung aufzubauen, überprüfen Sie, ob SSL-Scannen aktiviert ist während der Webfilter im Transparenzmodus arbeitet. Wenn das der Fall ist, stellen Sie sicher, dass der Zielhost der VPN-Verbindung zu den *Transparenzmodus-Ausnahmen* unter *Web Protection* > *Filteroptionen* > *Sonstiges* hinzugefügt wurde.

15.3.1 Verbindungen

Um einen SSL-VPN -Site-to-Site-Tunnel anzulegen, ist es entscheidend, zuerst die Serverkonfiguration anzulegen. Die Konfiguration des Clients muss immer erst der zweite Schritt sein.

Um eine Serverkonfiguration anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue SSL-Verbindung*.**
   Das Dialogfeld *SSL-Verbindung* hinzufügen wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Verbindungstyp: Wählen Sie *Server* aus der Auswahlliste aus.

   Verbindungsname: Geben Sie einen aussagekräftigen Namen für die Verbindung ein.

   Statische virtuelle IP-Adresse verwenden (optional): Wählen Sie diese Option nur, wenn der IP-Adressenpool nicht mit der Netzwerkumgebung des Clients kompatibel ist: Standardmäßig erhalten Clients eine IP-Adresse aus dem *Virtuellen IP-Pool* (konfigurierbar auf der Registerkarte *Einstellungen*). In Ausnahmefällen kann es passieren, dass eine solche IP-Adresse auf dem Host des Clients bereits in Benutzung ist.Geben Sie in diesem Fall eine passende IP-Adresse in das Feld *Statische Peer-IP* ein, welche daraufhin dem Client während des Tunnelaufbaus zugewiesen wird.

   Lokale Netzwerke: Wählen Sie eines oder mehrere lokale Netzwerke aus, die für den Fernzugriff zugelassen sein sollen bzw. fügen Sie es/sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   Entfernte Netzwerke: Wählen Sie eines oder mehrere Netzwerke der Gegenstelle aus, die sich mit dem/den lokalen Netzwerk(en) verbinden dürfen, bzw. fügen Sie es/sie hinzu.

   > **Hinweis –** Sie können die *lokalen Netzwerke* und die *entfernten Netzwerke* auch später noch konfigurieren, ohne dass Sie den Client neu konfigurieren müssten.

   Automatische Firewallregeln (optional): Wenn diese Option aktiviert ist, gewährt die UTM automatisch Zugriff auf die gewählten lokalen Netzwerke für alle SSL-VPN-Clients.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue SSL-Serververbindung wird in der Liste *Verbindungen* angezeigt.

4. **Laden Sie die Konfigurationsdatei herunter.**
   Klicken Sie auf die Schaltfläche *Download*, die sich im Feld der neuen SSL-Serververbindung befindet, um die Client-Konfigurationsdatei für diese Verbindung herunterzuladen.

Konfigurationsdatei verschlüsseln (optional): Es wird empfohlen, die Konfigurationsdatei aus Sicherheitsgründen zu verschlüsseln. Geben Sie ein Kennwort zweimal ein.
Klicken Sie auf *Peer-Konfig. herunterladen*, um die Datei zu speichern.
Diese Datei wird vom Administrator der Client-Seite benötigt, um in der Lage zu sein, den Client-Endpunkt des Tunnels zu konfigurieren.

Der nächste Schritt ist die Client-Konfiguration, die Client-seitig und *nicht* Server-seitig erfolgen muss.Stellen Sie sicher, dass die Client-Konfigurationsdatei bereitliegt.

Um eine Client-Konfiguration anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue SSL-Verbindung*.**
   Das Dialogfeld *SSL-Verbindung* hinzufügen wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Verbindungstyp: Wählen Sie *Client* aus der Auswahlliste aus.

   Verbindungsname: Geben Sie einen aussagekräftigen Namen für die Verbindung ein.

   Konfigurationsdatei: Klicken Sie auf das Ordnersymbol, wechseln Sie zur Client-Konfigurationsdatei und klicken Sie auf *Hochladen starten*.

   Kennwort (optional): Wenn die Datei verschlüsselt ist, geben Sie das Kennwort ein.

   HTTP-Proxy-Server verwenden (optional): Wählen Sie diese Option, wenn sich der Client hinter einem Proxy befindet, und geben Sie die Einstellungen für den Proxy ein.

      Proxy erfordert Authentifizierung (optional): Wählen Sie diese Option, wenn sich der Client am Proxy authentifizieren muss, und geben Sie Benutzername und Kennwort ein.

   Peer-Hostnamen übergehen (optional): Wählen Sie diese Option und geben Sie einen Hostnamen ein, wenn der reguläre Hostname des Serversystems (oder sein DynDNS-Hostname) nicht vom Clienthost aufgelöst werden kann.

   Automatische Firewallregeln (optional): Wenn diese Option aktiviert ist, lässt die UTM automatisch Verkehr zwischen Hosts der zum Tunnel gehörenden lokalen und entfernten Netzwerke zu.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue SSL-VPN-Clientverbindung wird in der Liste *Verbindungen* angezeigt.

Um eine Client-Verbindung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Klicken Sie auf den Menüpunkt *Site-to-Site-VPN*, um den Status der SSL-VPN-Verbindung auf der Übersichtsseite zu sehen. Die Statusampel dort wird grün, wenn die Verbindung aufgebaut ist. Dann werden auch Informationen zu den miteinander verbundenen Subnetzen beider Seiten des Tunnels angezeigt.

15.3.2 Einstellungen

Auf der Registerkarte *SSL > Einstellungen* können Sie die Grundeinstellungen für SSL-VPN-Serververbindungen konfigurieren.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN > SSL* und *Fernzugriff > SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

Servereinstellungen

Sie können die folgenden Einstellungen für die SSL-VPN-Verbindung vornehmen:

- **Schnittstellen-Adresse:** Der Standardwert lautet *Any*. Wenn Sie die Web Application Firewall verwenden, müssen Sie für diesen Dienst eine bestimmte Schnittstellenadresse angeben, die auf SSL-Verbindungen lauscht. Das ist für die Site-to-Site/Fernzugriff-SSL-Verbindungsverwaltung und die Web Application Firewall notwendig, damit diese die eingehenden SSL-Verbindungen auseinanderhalten können.
- **Protokoll:** Wählen Sie das Protokoll aus, das verwendet werden soll. Sie können entweder *TCP* oder *UDP* auswählen.
- **Port:** Sie können den Port ändern. Der Standardport ist `443`. Sie können jedoch nicht den Port `10443`, den SUM-Gateway-Manager-Port `4422` oder den Port der WebAdmin-Schnittstelle verwenden.
- **Hostnamen übergehen:** Der Wert im Feld *Hostnamen übergehen* wird als Zielhostname für Client-VPN-Verbindungen verwendet und ist standardmäßig der Hostname des Gateways. Ändern Sie den voreingestellten Wert nur, wenn der reguläre Hostname (oder DynDNS-Hostname) nicht unter diesem Namen aus dem Internet erreichbar ist.

Virtueller IP-Pool

Pool-Netzwerk: Das ist der virtuelle IP-Adressenpool, der verwendet wird, um IP-Adressen aus einem bestimmten IP-Adressbereich SSL-Clients zuzuweisen. Standardmäßig ist *VPN*

Pool (SSL) ausgewählt. Falls Sie einen anderen Adressenpool auswählen, darf die Netzmaske nicht größer als 29 Bit sein, da OpenVPN nicht mit Adressenpools umgehen kann, deren Netzmaske `/30`, `/31`, oder `/32` ist.

Doppelte CN

Wählen Sie *Mehrere gleichzeitige Verbindungen pro Benutzer zulassen*, wenn Sie zulassen wollen, dass Ihre Benutzer sich zur gleichen Zeit von verschiedenen IP-Adressen aus verbinden können. Wenn diese Option deaktiviert ist, ist nur eine gleichzeitige SSL-VPN-Verbindung pro Benutzer erlaubt.

15.3.3 Erweitert

Auf der Registerkarte *SSL* > *Erweitert* können Sie diverse erweiterte Serveroptionen konfigurieren, wie z. B. Einstellungen zur Kryptografie, zur Komprimierung und zur Fehlersuche.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN* > *SSL* und *Fernzugriff* > *SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

Kryptografische Einstellungen

Diese Einstellungen kontrollieren die Verschlüsselungsparameter für alle SSL- VPN -Fernzugriff-Clients:

- **Verschlüsselungsalgorithmus:** Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der Daten verwendet wird, die durch den VPN-Tunnel gesendet werden. Die folgenden Algorithmen werden unterstützt, welche alle im CBC-Modus *Cipher Block Chaining* sind:
  - *DES-EDE3-CBC*
  - *AES-128-CBC* (128 Bit)
  - *AES-192-CBC* (192 Bit)
  - *AES-256-CBC* (256 Bit)
  - *BF-CBC* (Blowfish (128 Bit))
- **Authentifizierungsalgorithmus:** Der Authentifizierungsalgorithmus legt den Algorithmus fest, der für die Integritätsprüfung der Daten verwendet wird, die durch den VPN-Tunnel gesendet werden. Die folgenden Algorithmen werden unterstützt:

    - *MD5* (128 Bit)
    - *SHA-1* (160 Bit)
    - *SHA2 256* (256 Bit)
    - *SHA2 384* (384 Bit)
    - *SHA2 512* (512 Bit)

- **Schlüssellänge:** Die Schlüssellänge ist die Länge des Diffie-Hellman-Schlüsselaustauschs. Je länger der Schlüssel ist, desto sicherer sind die symmetrischen Schlüssel. Die Länge wird in Bits angegeben. Sie können zwischen einer Schlüssellänge von 1024 und 2048 Bits wählen.
- **Serverzertifikat:** Wählen Sie ein lokales SSL-Zertifikat, das der SSL-VPN-Server verwenden soll, um sich gegenüber Clients zu identifizieren.
- **Schlüsselgültigkeit:** Geben Sie einen Zeitraum an, nach dem der Schlüssel abläuft. Standardmäßig sind 28.800 Sekunden voreingestellt.

Komprimierungseinstellungen

SSL-VPN-Verkehr komprimieren: Wenn diese Option aktiviert ist, werden alle Daten, die durch SSL-VPN-Tunnel geschickt werden, vor der Verschlüsselung komprimiert.

Fehlersuche-Einstellungen

Fehlersuche-Modus aktivieren: Wenn Sie den Fehlersuche-Modus aktivieren, enthält die SSL-VPN-Protokolldatei zusätzliche Informationen, die nützlich für die Fehlersuche sind.

15.4 Zertifikatverwaltung

Das Menü *Site-to-Site-VPN > Zertifikatverwaltung* ist der zentrale Ort, an dem alle zertifikatbezogenen Vorgänge verwaltet werden, die bei der Sophos UTM auftreten. Das beinhaltet unter anderem das Anlegen und Importieren von X.509-Zertifikaten sowie das Hochladen sogenannter *Zertifikatsperrlisten* (CRLs).

15.4.1 Zertifikate

Auf der Registerkarte *Site-to-Site-VPN > Zertifikatverwaltung > Zertifikate* können Sie öffentliche Schlüssel-Zertifikate im X.509-Standard erstellen oder importieren. Solche Zertifikate sind digital signierte Bescheinigungen, die üblicherweise von einer *Zertifizierungsstelle* (CA,

Certificate Authority) ausgestellt werden und einen öffentlichen Schlüssel mit einem bestimmten *Distinguished Name* (DN) in X.500-Schreibweise verknüpfen.

Alle Zertifikate, die Sie auf dieser Registerkarte erzeugen, enthalten einen RSA-Schlüssel.Sie sind von der selbst signierten Zertifizierungsstelle (CA) *VPN Signing CA* signiert, die automatisch mit den Informationen erstellt wurde, die Sie während der ersten Anmeldung am WebAdmin angegeben haben.

Um ein Zertifikat neu zu generieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zertifikate* auf *Neues Zertifikat*.**
   Das Dialogfeld *Zertifikat hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für dieses Zertifikat ein.

   Methode: Um ein Zertifikat zu erstellen, wählen Sie *Generieren* aus (weitere Informationen zum Hochladen von Zertifikaten finden Sie weiter unten).

   Schlüssellänge: Die Länge des RSA-Schlüssels. Je länger der Schlüssel, desto sicherer ist er. Sie können zwischen den Schlüssellängen 1024, 2048 oder 4096 Bit wählen. Verwenden Sie die größtmögliche Schlüssellänge, die mit Ihren Anwendungen und Ihrer Hardware kompatibel ist. Solange mit dem längeren Schlüssel keine kritischen Leistungsprobleme für Ihre spezifischen Zwecke auftreten, sollten Sie auf keinen Fall die Schlüssellänge reduzieren, um die Leistung zu optimieren.

   VPN-ID-Typ: Legen Sie eine einzigartige Identifikation (identifier) für das Zertifikat fest. Die folgenden Identifikationsarten sind verfügbar:

   - E-Mail-Adresse
   - Hostname
   - IP-Adresse
   - Distinguished Name

   VPN-ID: Tragen Sie abhängig von der gewählten Identifikationsart (VPN-ID) den passenden Wert in das Feld ein. Beispiel: Wenn Sie in der Auswahlliste *VPN-ID-TypIP-Adresse* gewählt haben, geben Sie eine IP-Adresse in dieses Textfeld ein. Beachten Sie, dass dieses Textfeld verborgen ist, wenn Sie in der Auswahlliste *VPN-ID-TypDistinguished Name* gewählt haben.

Verwenden Sie die Auswahllisten und Textfelder *Land* bis *E-Mail*, um die Informationen zum Zertifikatsinhaber einzutragen. Diese Informationen werden dazu verwendet, den *Distinguished Name* zu erstellen, d. h. den Namen der Instanz, deren öffentlichen Schlüssel das Zertifikat identifiziert. Dieser Name enthält viele persönliche Informationen im X.500-Standard, weswegen davon ausgegangen wird, dass dieser Name im gesamten Internet einzigartig ist. Falls das Zertifikat für eine Road-Warrior-Verbindung verwendet wird, geben Sie den Namen des Benutzers in das Feld *Allgemeiner Name* ein. Wenn das Zertifikat für einen Host ist, geben Sie einen Hostnamen ein.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Das Zertifikat wird in der Liste *Zertifikate* angezeigt.

Um ein Zertifikat zu löschen, klicken Sie auf die Schaltfläche *Löschen* des entsprechenden Zertifikats.

Um alternativ ein Zertifikat hochzuladen (zu importieren), gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zertifikate* auf *Neues Zertifikat*.**
   Das Dialogfeld *Zertifikat hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für dieses Zertifikat ein.

   Methode: Um ein Zertifikat zu importieren, wählen Sie *Hochladen* aus.

   Dateityp: Wählen Sie den Dateityp des Zertifikats aus. Sie können Zertifikate der folgenden Dateitypen hochladen:

   - **PKCS#12 (Zert.+CA):** PKCS bezieht sich auf eine Gruppe von *Public Key Cryptography Standards* (dt. etwa Standards für die Kryptografie öffentlicher Schlüssel), die von den RSA Laboratories entwickelt und veröffentlicht wurden. Das Dateiformat `PKCS#12` wird gemeinhin dafür benutzt, private Schlüssel mit dem zugehörigen öffentlichen Schlüsselzertifikat zu speichern und mit einem Kennwort zu schützen. Sie müssen dieses Container-Kennwort kennen, um Dateien in diesem Format hochladen zu können.

   - **PEM (nur Zert.):** Ein Base64-codiertes Format (*Privacy Enhanced Mail*, `PEM`), das kein Kennwort erfordert.

Datei: Klicken Sie auf das Ordnersymbol neben dem Feld *Datei* und wählen Sie das Zertifikat aus, das hochgeladen werden soll.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Das Zertifikat wird in der Liste *Zertifikate* angezeigt.

Um ein Zertifikat zu löschen, klicken Sie auf die Schaltfläche *Löschen* des entsprechenden Zertifikats.

Sie können das Zertifikat entweder im `PKCS#12`- oder `PEM`-Format herunterladen. Die `PEM`-Datei enthält nur das Zertifikat selbst, wohingegen die `PKCS#12`-Datei auch noch den privaten Schlüssel sowie das CA-Zertifikat enthält, mit dem das Zertifikat signiert wurde.

15.4.2 Certificate Authority (Zertifizierungsstelle)

Auf der Registerkarte *Site-to-Site-VPN > Zertifikatverwaltung > CA* können Sie neue *Zertifizierungsstellen* importieren. Eine Zertifizierungsstelle (CA, *Certificate Authority*) ist eine Organisation, die digitale Zertifikate für die Benutzung durch andere Parteien ausstellt. Eine CA attestiert, dass der im Zertifikat enthaltene öffentliche Schlüssel zur Person oder Organisation, zum Host oder einer anderen Instanz gehört, die/der im Zertifikat aufgeführt ist. Dies wird erreicht, indem bei der Signierungsanfrage das Zertifikat mit dem privaten Schlüssel des CA-eigenen Zertifikats signiert wird.Solch eine CA wird deshalb auch als Signierungs-CA bezeichnet.

Auf der UTM wurde die Signierungs-CA automatisch während der ersten Anmeldung an der UTM generiert, wobei die angegebenen Informationen verwendet wurden. Dadurch sind alle Zertifikate, die Sie auf der Registerkarte *Zertifikate* erzeugen, selbst-signierte Zertifikate, das bedeutet, dass Aussteller und Inhaber identisch sind. Alternativ können Sie jedoch eine Signierungs-CA eines Drittanbieters importieren. Darüber hinaus können Sie auch andere CA-Zertifikate verwenden, deren private Schlüssel unbekannt sind, um die Authentizität eines Hosts oder Benutzers zu überprüfen, der versucht, sich über IPsec zu verbinden. Diese CA-Zertifikate wiederum werden als Verifizierungs-CAs bezeichnet und können auch auf dieser Registerkarte importiert werden.

Wichtiger Hinweis – Auf Ihrem System können mehrere Verifizierungs-CAs vorhanden sein, allerdings nur eine Signierungs-CA. Wenn Sie also eine neue Signierungs-CA hoch-

laden, wird die zuvor installierte Signierungs-CA automatisch in eine Verifizierungs-CA umgewandelt.

Um eine CA zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *CA* auf *CA importieren*.**
   Das Dialogfeld *CA importieren* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese CA ein.

   Typ: Wählen Sie den CA-Typ, den Sie importieren werden. Sie können zwischen Verifizierungs-CA und Signierungs-CA wählen. Eine Verifizierungs-CA muss im `PEM`-Format vorliegen, wohingegen eine Signierungs-CA im `PKCS#12`-Format vorliegen muss.

   CA-Zertifikat: Klicken Sie auf das Ordner-Symbol neben dem Feld *CA-Zertifikat* und wählen Sie die zu importierende Datei aus. Wenn Sie eine neue Signierungs-CA hochladen, beachten Sie, dass Sie das Kennwort eingeben müssen, mit dem der `PKCS#12`-Container gesichert wurde.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.
3. **Klicken Sie auf *Speichern*.**
   Das neue CA-Zertifikat wird in der Liste *CA* angezeigt.

Um eine CA zu löschen, klicken Sie auf die Schaltfläche *Löschen* der entsprechenden CA.

Die Signierungs-CA kann im `PKCS#12`-Format heruntergeladen werden. Sie werden daraufhin aufgefordert, ein Kennwort einzugeben, das zur Sicherung des `PKCS#12`-Containers benutzt wird. Außerdem können Sie Verifizierungs-CAs im `PEM`-Format herunterladen.

15.4.3 Sperrlisten (CRLs)

Eine Zertifikatsperrliste (CRL, Certificate Revocation List; auch Widerrufsliste) ist eine Liste von Zertifikaten (genauer: ihren Seriennummern), die widerrufen wurden, d. h. nicht mehr gültig und aus diesem Grund nicht vertrauenswürdig sind. Auf der Registerkarte *Site-to-Site-VPN > Zertifikatverwaltung > Sperrlisten (CRLs)* können Sie eine Zertifikatsperrliste importieren, die sich auf Ihre Public-Key-Infrastruktur (PKI, dt. Infrastruktur für öffentliche Schlüssel) bezieht.

Um eine Zertifikatsperrliste (CRL) hochzuladen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Sperrlisten (CRLs)* auf *CRL hochladen*.**
   Das Dialogfeld *CRL hochladen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese CRL ein.

   CRL-Datei: Klicken Sie auf das Ordner-Symbol neben dem Feld *CRL-Datei* und wählen Sie die zu importierende Datei aus.

   Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue CRL wird in der Liste der Sperrlisten angezeigt.

Um eine Sperrliste zu löschen, klicken Sie auf die Schaltfläche *Löschen* der entsprechenden Sperrliste.

15.4.4 Erweitert

Auf der Registerkarte *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Erweitert* können Sie die VPN-Signierungs-CA neu generieren, die während der ersten Anmeldung am Sicherheitssystem automatisch generiert wurde. Mit der VPN-Signierungs-CA werden die Zertifikate für die Fernzugriffs- und Site-to-Site-VPN-Verbindungen digital signiert. Die alte VPN-Signierungs-CA wird als Verifizierungs-CA beibehalten.

Signierungs-CA neu erstellen

Sie können alle Benutzerzertifikate mit der aktuellen Signierungs-CA erneuern. Das wird dann notwendig, wenn Sie eine alternative VPN-Signierungs-CA auf der Registerkarte *CA* installiert haben.

Warnung – Die UTM- und alle Benutzerzertifikate werden mit der neuen Signierungs-CA neu generiert. Dies unterbricht zertifikatbasierte Site-to-Site- und Fernzugriffsverbindungen.

16 Fernzugriff

In diesem Kapitel wird beschrieben, wie Sie den Fernzugriff (Remote Access) für die Sophos UTM konfigurieren. Der Fernzugriff wird in Sophos UTM mittels *virtuellen privaten Netzwerken* (Virtual Private Networks (VPNs)), realisiert. Diese sind ein kostengünstiger und sicherer Weg, entfernten Benutzern wie Angestellten, die von unterwegs und von zu Hause aus arbeiten, den Zugang zum Firmennetzwerk zu ermöglichen. VPNs verwenden kryptografische Tunnelprotokolle wie IPsec und PPTP, um Vertraulichkeit und Datenschutz für die übertragenen Daten zu gewährleisten.

Querverweis – Weitere Informationen zur Konfiguration von Fernzugriff-VPN-Verbindungen finden Sie in der Sophos-Knowledgebase.

Die UTM generiert automatisch die notwendigen Installations- und Konfigurationsdateien für die jeweilige Verbindungsart des Fernzugriffs. Diese Dateien können direkt über das Benutzerportal heruntergeladen werden. Für jeden Benutzer sind jedoch nur diejenigen Dateien verfügbar, die den für ihn aktivierten Verbindungsarten entsprechen. Beispiel: Ein Benutzer, für den der SSL-Fernzugriff aktiviert ist, findet nur eine SSL-Installationsdatei vor.

Hinweis – Sie können die Konfigurationsdateien für den Fernzugriff für alle oder ausgewählte Benutzer über die Registerkarte *Definitionen & Benutzer > Benutzer & Gruppen > Benutzer* herunterladen.

Die Seite *Fernzugriffsstatus* enthält eine Übersicht mit allen Online-Benutzern.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- SSL
- PPTP
- L2TP über IPsec
- IPsec
- HTML5-VPN-Portal
- Cisco VPN Client

- Erweitert
- Zertifikatverwaltung

16.1 SSL

Die Fernzugriff-SSL-Funktion von Sophos UTM wird durch OpenVPN realisiert, einer umfassenden SSL-VPN-Lösung. Sie bietet die Möglichkeit, zwischen entfernten Mitarbeitern und dem Unternehmensnetzwerk Punkt-zu-Punkt-verschlüsselte Tunnel aufzubauen, wobei SSL-Zertifikate und eine Benutzer-Kennwort-Kombination benötigt werden, um sich für den Zugriff auf interne Ressourcen zu authentifizieren. Zusätzlich bietet es ein sicheres Benutzerportal, das von jedem autorisierten Benutzer erreicht werden kann, um ein maßgeschneidertes SSL-VPN-Client-Software-Paket herunterzuladen. Dieses Paket beinhaltet einen kostenlosen SSL-VPN-Client, SSL-Zertifikate und eine Konfiguration, die sich über ein einfaches Installationsverfahren mit nur einem Mausklick durchführen lässt. Der SSL-VPN-Client unterstützt die gängigsten Geschäftsanwendungen wie natives Outlook, native Windows-Dateifreigabe und viele weitere.

Querverweis – Weitere Informationen zur Nutzung des SSL-VPN-Clients finden Sie in der Sophos-Knowledgebase.

16.1.1 Profile

Auf der Registerkarte *Fernzugriff* > *SSL* > *Profile* können Sie für Fernzugriffbenutzer verschiedene Profile mit den Grundeinstellungen für den SSL-VPN-Zugang anlegen.

Um ein SSL-VPN-Profil anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Profile* auf *Neues Fernzugriffsprofil*.**
   Das Dialogfeld *Neues Fernzugriffsprofil* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Profilname: Geben Sie einen aussagekräftigen Namen für das Profil ein.

   Benutzer und Gruppen: Wählen Sie die für den SSL-VPN-Fernzugriff mit diesem Profil zugelassenen Benutzer und Benutzergruppen aus oder fügen Sie neue Benutzer und Benutzergruppen hinzu. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer* erläutert.

Lokale Netzwerke: Legen Sie die lokalen Netzwerke fest, die für die ausgewählten SSL-VPN-Clients über den VPN-SSL-Tunnel erreichbar sein sollen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

> **Hinweis –** Standardmäßig setzt die SSL-VPN-Lösung von Sophos UTM sogenanntes Split Tunneling (dt. etwa geteiltes Tunneln) ein. Das bedeutet, dass ein entfernter VPN-Benutzer Zugang zu einem öffentlichen Netzwerk (z. B. dem Internet) hat und gleichzeitig auf Ressourcen im VPN zugreifen kann. Split Tunneling kann jedoch auch umgangen werden, indem Sie im Feld *Lokale Netzwerke* die Option *Any* auswählen. Dadurch wird der gesamte Verkehr durch den VPN-SSL-Tunnel geroutet. Ob Benutzer dann noch auf ein öffentliches Netzwerk zugreifen dürfen oder nicht, hängt von Ihren Firewall-Einstellungen ab.

Automatische Firewallregeln: Wählen Sie diese Option, um automatisch Firewallregeln hinzuzufügen, die Verkehr für dieses Profil erlauben. Die Regeln werden hinzugefügt, sobald das Profil aktiv ist, und sie werden gelöscht, wenn das Profil deaktiviert wird. Wenn Sie diese Option nicht auswählen, müssen Sie entsprechende Firewallregeln manuell anlegen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Das neue Profil wird in der Liste *Profile* angezeigt.

Um ein Profil zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

> **Hinweis –** Das Menü *Fernzugriff* im Benutzerportal ist nur für Benutzer verfügbar, die im Feld *Benutzer und Gruppen* ausgewählt wurden *und* für die eine Benutzerdefinition auf der UTM existiert (siehe *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer*). Autorisierte Benutzer finden nach dem Einloggen in das Benutzerportal das SSL-VPN-Client-Softwarepaket sowie einen Link zu einer Installationsanleitung in der Sophos-Knowledgebase. Das Herunterladen kann mit einigen Browsern auf Android fehlschlagen, wenn das CA-Zertifikat nicht installiert ist oder wenn der Hostname nicht mit dem allgemeinen Namen (engl. common name) im Portal-Zertifikat übereinstimmt. In diesem Fall muss der Benutzer das CA-Zertifikat installieren oder einen anderen Browser verwenden.

Live-Protokoll öffnen

Im *OpenVPN-Live-Protokoll* werden die Fernzugriff-Aktivitäten protokolliert. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

16.1.2 Einstellungen

Auf der Registerkarte *SSL > Einstellungen* können Sie die Grundeinstellungen für SSL-VPN-Serververbindungen konfigurieren.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN > SSL* und *Fernzugriff > SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

Servereinstellungen

Sie können die folgenden Einstellungen für die SSL-VPN-Verbindung vornehmen:

- **Schnittstellen-Adresse:** Der Standardwert lautet *Any*. Wenn Sie die Web Application Firewall verwenden, müssen Sie für diesen Dienst eine bestimmte Schnittstellenadresse angeben, die auf SSL-Verbindungen lauscht. Das ist für die Site-to-Site/Fernzugriff-SSL-Verbindungsverwaltung und die Web Application Firewall notwendig, damit diese die eingehenden SSL-Verbindungen auseinanderhalten können.
- **Protokoll:** Wählen Sie das Protokoll aus, das verwendet werden soll. Sie können entweder *TCP* oder *UDP* auswählen.
- **Port:** Sie können den Port ändern. Der Standardport ist `443`. Sie können jedoch nicht den Port `10443`, den SUM-Gateway-Manager-Port `4422` oder den Port der WebAdmin-Schnittstelle verwenden.
- **Hostnamen übergehen:** Der Wert im Feld *Hostnamen übergehen* wird als Zielhostname für Client-VPN-Verbindungen verwendet und ist standardmäßig der Hostname des Gateways. Ändern Sie den voreingestellten Wert nur, wenn der reguläre Hostname (oder DynDNS-Hostname) nicht unter diesem Namen aus dem Internet erreichbar ist.

Virtueller IP-Pool

Pool-Netzwerk: Das ist der virtuelle IP-Adressenpool, der verwendet wird, um IP-Adressen aus einem bestimmten IP-Adressbereich SSL-Clients zuzuweisen. Standardmäßig ist *VPN Pool (SSL)* ausgewählt. Falls Sie einen anderen Adressenpool auswählen, darf die Netzmaske

nicht größer als 29 Bit sein, da OpenVPN nicht mit Adressenpools umgehen kann, deren Netzmaske `/30`, `/31`, oder `/32` ist.

Doppelte CN

Wählen Sie *Mehrere gleichzeitige Verbindungen pro Benutzer zulassen*, wenn Sie zulassen wollen, dass Ihre Benutzer sich zur gleichen Zeit von verschiedenen IP-Adressen aus verbinden können. Wenn diese Option deaktiviert ist, ist nur eine gleichzeitige SSL-VPN-Verbindung pro Benutzer erlaubt.

16.1.3 Erweitert

Auf der Registerkarte *SSL* > *Erweitert* können Sie diverse erweiterte Serveroptionen konfigurieren, wie z. B. Einstellungen zur Kryptografie, zur Komprimierung und zur Fehlersuche.

> **Hinweis –** Diese Registerkarte ist identisch für *Site-to-Site-VPN* > *SSL* und *Fernzugriff* > *SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

Kryptografische Einstellungen

Diese Einstellungen kontrollieren die Verschlüsselungsparameter für alle SSL- VPN -Fernzugriff-Clients:

- **Verschlüsselungsalgorithmus:** Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der Daten verwendet wird, die durch den VPN-Tunnel gesendet werden. Die folgenden Algorithmen werden unterstützt, welche alle im CBC-Modus *Cipher Block Chaining* sind:
  - *DES-EDE3-CBC*
  - *AES-128-CBC* (128 Bit)
  - *AES-192-CBC* (192 Bit)
  - *AES-256-CBC* (256 Bit)
  - *BF-CBC* (Blowfish (128 Bit))
- **Authentifizierungsalgorithmus:** Der Authentifizierungsalgorithmus legt den Algorithmus fest, der für die Integritätsprüfung der Daten verwendet wird, die durch den VPN-Tunnel gesendet werden. Die folgenden Algorithmen werden unterstützt:
  - *MD5* (128 Bit)
  - *SHA-1* (160 Bit)

- *SHA2 256* (256 Bit)
- *SHA2 384* (384 Bit)
- *SHA2 512* (512 Bit)

- **Schlüssellänge:** Die Schlüssellänge ist die Länge des Diffie-Hellman-Schlüsselaustauschs. Je länger der Schlüssel ist, desto sicherer sind die symmetrischen Schlüssel. Die Länge wird in Bits angegeben. Sie können zwischen einer Schlüssellänge von 1024 und 2048 Bits wählen.
- **Serverzertifikat:** Wählen Sie ein lokales SSL-Zertifikat, das der SSL-VPN-Server verwenden soll, um sich gegenüber Clients zu identifizieren.
- **Schlüsselgültigkeit:** Geben Sie einen Zeitraum an, nach dem der Schlüssel abläuft. Standardmäßig sind 28.800 Sekunden voreingestellt.

Komprimierungseinstellungen

SSL-VPN-Verkehr komprimieren: Wenn diese Option aktiviert ist, werden alle Daten, die durch SSL-VPN-Tunnel geschickt werden, vor der Verschlüsselung komprimiert.

Fehlersuche-Einstellungen

Fehlersuche-Modus aktivieren: Wenn Sie den Fehlersuche-Modus aktivieren, enthält die SSL-VPN-Protokolldatei zusätzliche Informationen, die nützlich für die Fehlersuche sind.

16.2 PPTP

PPTP (Point-to-Point Tunneling Protocol) ermöglicht einzelnen Hosts mit Hilfe eines verschlüsselten Tunnels den Zugriff über das Internet auf interne Netzwerkdienste. PPTP ist einfach einzurichten und benötigt auf Microsoft Windows-Systemen keine spezielle Software.

PPTP ist in Microsoft Windows ab Version 95 enthalten. Um PPTP mit Sophos UTM verwenden zu können, muss der Client das MSCHAPv2-Authentifizierungsprotokoll unterstützen. Benutzer von Windows 95 und 98 müssen ein Update aufspielen, damit dieses Protokoll unterstützt wird.

16.2.1 Allgemein

Um die allgemeinen Optionen für PPTP zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den PPTP-Fernzugriff auf der Registerkarte *Allgemein*.**
Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Haupteinstellungen* kann bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
Authentifizierung über: Wählen Sie die Authentifizierungsmethode. PPTP-Fernzugriff unterstützt nur die lokale und die RADIUS-Authentifizierung.

   - **Lokal:** Wenn Sie *Lokal* wählen, geben Sie die Benutzer und Benutzergruppen an, die sich per PPTP-Fernzugriff verbinden dürfen. Es ist nicht möglich, Backend-Benutzergruppen in das Feld zu ziehen. Solange kein Benutzerkonto ausgewählt ist, kann der PPTP-Fernzugriff nicht eingeschaltet werden.

     Hinweis – Benutzername und Kennwort der gewählten Benutzer dürfen nur druckbare ASCII-Zeichen enthalten[1].

     Hinweis – Ähnlich wie bei SSL-VPN steht das Menü *Fernzugriff* des Benutzerportals nur Benutzern zur Verfügung, die im Feld *Benutzer und Gruppen* ausgewählt sind und für die in der UTM eine Benutzerdefinition existiert. Autorisierte Benutzer, die sich erfolgreich am Benutzerportal angemeldet haben, finden einen Link zu einer Installationsanleitung in der Sophos-Knowledgebase.

   - **RADIUS:** *RADIUS* kann nur ausgewählt werden, wenn zuvor ein RADIUS-Server konfiguriert wurde. Bei dieser Authentifizierungsmethode werden Benutzer an einem externen RADIUS-Server authentifiziert, welcher auf der Registerkarte *Definitionen & Benutzer* > *Authentifizierungsdienste* > *Server* konfiguriert werden kann. Das Dialogfeld *Benutzer und Gruppen* wird dann ausgegraut; seine Einstellungen können zwar noch geändert werden, haben aber keinen Effekt mehr. Der RADIUS-Server muss MSCHAPv2-Challenge-Response-Authentifizierung unterstützen. Der Server kann Parameter wie die Client-IP-Adresse und die DNS/WINS-Serveradressen zurückgeben. Das PPTP-Modul sendet die folgende NAS-ID an den RADIUS-Server: `pptp`. Wenn RADIUS-Authentifizierung gewählt ist, beachten Sie, dass lokale Benutzer nicht länger mit PPTP authentifiziert wer-

[1] http://de.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

den können. Des Weiteren müssen auch Clients die MSCHAPv2-Authentifizierung unterstützen.

IP-Adressen zuweisen durch: IP-Adressen können Sie entweder aus einem festgelegten IP-Adressenpool zuweisen oder von einem DHCP-Server automatisch verteilen lassen:

- **IP-Adressenpool:** Wählen Sie diese Option aus, wenn Sie IP-Adressen aus einem bestimmten IP-Adressbereich an Clients zuweisen wollen, die sich per Fernzugriff über PPTP verbinden. Standardmäßig werden Adressen aus dem privaten IP-Raum `10.242.1.0/24` zugewiesen. Diese Netzwerkdefinition heißt *VPN Pool (PPTP)* und kann in allen Netzwerk-spezifischen Konfigurationsoptionen verwendet werden. Wenn Sie ein anderes Netzwerk verwenden möchten, ändern Sie einfach die Definition von *VPN Pool (PPTP)* auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen*. Alternativ können Sie auch einen anderen IP-Adressenpool anlegen, indem Sie auf das Plussymbol neben dem Textfeld *Pool-Netzwerk* klicken.
- **DHCP-Server:** Wenn Sie *DHCP-Server* auswählen, geben Sie auch die Netzwerkschnittstelle an, über die der DHCP-Server erreichbar ist. Der DHCP-Server muss nicht direkt mit der Schnittstelle verbunden sein – der Zugriff ist auch über einen Router möglich. Beachten Sie, dass der lokale DHCP-Server nicht unterstützt wird; der hier gewählte DHCP-Server muss auf einem physikalisch anderen System laufen.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Live-Protokoll

Im *PPTP-Daemon-Live-Protokoll* werden die Aktivitäten des PPTP-Fernzugriffs protokolliert. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

16.2.2 iOS-Geräte

Sie können ermöglichen, dass Benutzern von iOS-Geräten eine automatische PPTP-Konfiguration im Benutzerportal angeboten wird.

Allerdings werden nur Benutzer, die im Feld *Benutzer und Gruppen* auf der Registerkarte *Allgemein* aufgeführt sind, die Konfigurationsdateien auf ihrer Benutzerportal-Seite finden. Der iOS-Geräte-Status ist standardmäßig aktiviert.

Verbindungsname: Geben Sie einen aussagekräftigen Namen für die PPTP-Verbindung ein, sodass iOS-Benutzer die Verbindung identifizieren können, die sie im Begriff sind, aufzubauen.Der Name Ihrer Firma gefolgt vom Protokoll PPTP ist voreingestellt.

Hinweis – *Der Verbindungsname* muss für alle iOS-Verbindungseinstellungen (PPTP, L2TP-over-IPsec, Cisco VPN Client) eindeutig sein.

Hostnamen übergehen: Im Falle, dass der Systemhostname vom Client nicht öffentlich aufgelöst werden kann, können Sie hier einen Server-Hostnamen eingeben, der die interne Präferenz übergeht, bei der der *DynDNS-Hostname* dem *System-DNS-Hostnamen* vorgezogen wird.

Um die automatische iOS-Geräte-Konfiguration zu deaktivieren, klicken Sie auf den Schieberegler.

Der Schieberegler wird grau.

16.2.3 Erweitert

Auf der Registerkarte *Fernzugriff > PPTP > Erweitert* können Sie die Verschlüsselungsstärke und die Menge an Fehlersuchemeldungen für PPTP-Fernzugriff konfigurieren. Die erweiterten PPTP-Einstellungen können nur konfiguriert werden, wenn PPTP auf der Registerkarte *Allgemein* aktiviert ist.

Verschlüsselungsstärke

Sie können zwischen einer starken (128 Bit) und einer schwachen (40 Bit) Tunnel-Verschlüsselung (MPPE) wählen. Verwenden Sie nach Möglichkeit nicht die schwache Verschlüsselung, außer Sie haben Gegenstellen, die die 128-Bit-Verschlüsselung nicht unterstützen.

Fehlersuche-Modus

Fehlersuche-Modus aktivieren: Diese Option kontrolliert die Menge an Fehlersuchemeldungen, die im PPTP-Protokoll erzeugt wird. Aktivieren Sie diese Option, wenn Sie Verbindungsprobleme haben und detaillierte Informationen über beispielsweise die Aushandlung der Client-Parameter benötigen.

16.3 L2TP über IPsec

L2TP ist die Kurzform für *Layer 2 Tunneling Protocol* und ist ein Datenlink-Ebene-Protokoll (Ebene 2 des OSI-Modells) für das Tunneln von Netzwerkverkehr zwischen zwei Peers über ein existierendes Netzwerk (meistens das Internet), auch bekannt als Virtuelles Privates Netzwerk (Virtual Private Network, VPN). Da das L2TP-Protokoll allein keine Vertraulichkeit mitbringt, wird es oft mit IPsec kombiniert, das Vertraulichkeit, Authentifizierung und Integrität bietet. Die Kombination dieser beiden Protokolle ist auch als L2TP über IPsec bekannt (engl. L2TP over IPsec). Mit L2TP über IPsec können Sie mit der gleichen Funktionalität wie PPTP einzelnen Hosts über einen verschlüsselten IPsec-Tunnel den Zugang zum Unternehmensnetzwerk ermöglichen.

16.3.1 Allgemein

Auf der Registerkarte *L2TP-over-IPsec* > *Allgemein* können Sie die grundlegenden Optionen für den Fernzugriff über L2TP-over-IPsec konfigurieren.

Um L2TP über IPsec zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie L2TP über IPsec auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Servereinstellungen und IP-Adressenzuweisung* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Schnittstelle: Wählen Sie die Netzwerkschnittstelle, die für den L2TP-VPN-Zugang verwendet werden soll.

   Authentifizierungsmodus: Sie können zwischen den folgenden Authentifizierungsmethoden wählen:

   - **Verteilter Schlüssel:** Geben Sie ein Kennwort ein, das als verteilter Schlüssel dient. Die Authentifizierung mit *verteilten Schlüsseln* (PSK, engl. preshared keys) erfolgt durch Schlüssel mit einem geheimen Kennwort, die vor der eigentlichen Verbindung unter den Beteiligten ausgetauscht werden. Um zu kommunizieren, weisen beide Gegenstellen nach, dass sie den vereinbarten Schlüssel kennen. Der vereinbarte Schlüssel ist ein Kennwort, das dazu benutzt wird, den

Datenverkehr mit dem Verschlüsselungsalgorithmus von L2TP zu verschlüsseln. Um die höchstmögliche Sicherheit zu gewährleisten, sollten Sie sich an den gängigen Maßstäben für die Stärke des Kennwortes orientieren. Wie sicher solche vereinbarten Schlüssel sind, hängt davon ab, wie sicher das Kennwort gewählt wurde und wie sicher es übertragen wurde. Kennwörter, die aus allgemeinen Wörtern bestehen, sind sehr anfällig für Wörterbuchangriffe. Daher sollte ein Kennwort ziemlich lang sein und eine Reihe von Buchstaben, Großbuchstaben und Zahlen enthalten. Folglich sollte ein verteilter Schlüssel auch nicht als Authentifizierungsmethode verwendet, sondern durch Zertifikate ersetzt werden, wo immer dies möglich ist.

> **Hinweis –** Wenn Sie den Zugang für iOS-Geräte ermöglichen wollen, müssen Sie *Verteilter Schlüssel* wählen, da iOS-Geräte nur PSK-Authentifizierung unterstützen.

- **X.509-CA-Prüfung:** Die Authentifizierung durch X.509-Zertifikate erleichtert den Austausch des öffentlichen Schlüssels in großen VPN-Installationen mit vielen Teilnehmern. Eine sogenannte CA (engl. Certificate Authority, Zertifizierungsstelle) erfasst und überprüft die öffentlichen Schlüssel der VPN-Endpoints und stellt für jeden Teilnehmer ein Zertifikat aus. Dieses Zertifikat enthält Informationen zur Identität des Teilnehmers und den zugehörigen öffentlichen Schlüssel. Da das Zertifikat digital signiert ist, kann niemand anderes ein gefälschtes Zertifikat verteilen, ohne entdeckt zu werden.
  Während des Schlüsselaustauschs werden die X.509-Zertifikate ausgetauscht und mit Hilfe der lokal installierten CAs beglaubigt. Die eigentliche Authentifizierung der VPN-Endpoints wird dann durch die öffentlichen und privaten Schlüssel durchgeführt. Wenn Sie diese Authentifizierungsmethode verwenden wollen, wählen Sie ein X.509-Zertifikat.
  Beachten Sie, dass Sie für die X.509-Authentifizierungsmethode auf der Registerkarte *Fernzugriff > Zertifikatverwaltung >* Zertifizierungsstelle eine gültige CA konfiguriert haben müssen.

IP-Adressen zuweisen durch: IP-Adressen können Sie entweder aus einem festgelegten IP-Adressenpool zuweisen oder von einem DHCP-Server automatisch verteilen lassen:

- **Pool-Netzwerk:** Standardmäßig ist *IP-Adressenpool* für die IP-Adressenzuweisung ausgewählt, wobei die Netzwerkdefinition *VPN Pool (L2TP)* als

Pool-Netzwerk voreingestellt ist.Der *VPN Pool (L2TP)* ist ein zufällig generiertes Netzwerk aus dem IP-Adressbereich `10.x.x.x` für private Netzwerke, für das ein Klasse-C-Subnetz verwendet wird. Normalerweise ist es nicht notwendig, das zu ändern, da es sicherstellt, dass die Benutzer einen bestimmten Adressenpool haben, von dem aus sie Verbindungen aufbauen können.Wenn Sie ein anderes Netzwerk verwenden wollen, können Sie einfach die Definition des *VPN Pools (L2TP)* ändern oder hier ein anderes Netzwerk als IP-Adressenpool angeben.

Hinweis – Wenn Sie private IP-Adressen für Ihren L2TP-VPN-Pool verwenden und wollen, dass IPsec-Hosts auf das Internet zugreifen dürfen, legen Sie entsprechende Maskierungs- oder NAT-Regeln für den IP-Adressenpool an.

- **DHCP-Server:** Wenn Sie *DHCP-Server* auswählen, geben Sie auch die Netzwerkschnittstelle an, über die der DHCP-Server erreichbar ist. Der DHCP-Server muss nicht direkt mit der Schnittstelle verbunden sein – der Zugriff ist auch über einen Router möglich. Beachten Sie, dass der lokale DHCP-Server nicht unterstützt wird; der hier gewählte DHCP-Server muss auf einem physikalisch anderen System laufen.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

   Um die Konfiguration abzubrechen, klicken Sie auf den gelben Schieberegler.

Zugriffskontrolle

Authentifizierung über: L2TP-Fernzugriff unterstützt nur die lokale und RADIUS-Authentifizierung.

- **Lokal:** Wenn Sie *Lokal* wählen, geben Sie die Benutzer und Benutzergruppen an, die sich per L2TP-Fernzugriff verbinden dürfen. Es ist nicht möglich, Backend-Benutzergruppen in das Feld zu ziehen. Lokale Benutzer müssen Sie auf dem herkömmlichen Weg hinzufügen und L2TP für sie aktivieren. Wenn keine Benutzer oder Gruppen ausgewählt sind, wird L2TP-Fernzugriff ausgeschaltet. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer* erläutert.

> **Hinweis –** Benutzername und Kennwort der gewählten Benutzer dürfen nur druckbare ASCII-Zeichen enthalten[1].

> **Hinweis –** Ähnlich wie bei SSL-VPN steht das Menü *Fernzugriff* des Benutzerportals nur Benutzern zur Verfügung, die im Feld *Benutzer und Gruppen* ausgewählt sind und für die in der UTM eine Benutzerdefinition existiert. In Abhängigkeit von der Authentifizierungsmethode liegt für autorisierte Benutzer, die sich erfolgreich am Benutzerportal angemeldet haben, der verteilte Schlüssel für IPsec (Authentifizierungsmethode *Verteilter Schlüssel*) oder die Datei `PKCS#12` (Authentifizierungsmethode *X.509-CA-Prüfung*) sowie ein Link zur Installationsanleitung bereit, die in der Sophos-Knowledgebase zur Verfügung steht.

- **RADIUS:** Wenn Sie *RADIUS*, auswählen, werden die Authentifizierungsanfragen an den RADIUS-Server weitergeleitet. Das L2TP-Modul sendet folgende Zeichenfolge als NAS-ID an den RADIUS-Server: `l2tp`.

Der Authentifizierungsalgorithmus wird automatisch zwischen dem Client und dem Server ausgehandelt. Für lokale Benutzer unterstützt Sophos UTM die folgenden Authentifizierungsprotokolle:

- MSCHAPv2
- PAP

Standardmäßig handelt ein Windows-Client MSCHAPv2 aus.

Für RADIUS-Benutzer unterstützt Sophos UTM folgende Authentifizierungsprotokolle:

- MSCHAPv2
- MSCHAP
- CHAP
- PAP

[1] http://de.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

16.3.2 iOS-Geräte

Sie können ermöglichen, dass Benutzern von iOS-Geräten eine automatische L2TP-über-IPsec-Konfiguration im Benutzerportal angeboten wird.

Allerdings werden nur Benutzer, die im Feld *Benutzer und Gruppen* auf der Registerkarte *Allgemein* aufgeführt sind, die Konfigurationsdateien auf ihrer Benutzerportal-Seite finden. Der iOS-Geräte-Status ist standardmäßig aktiviert.

Verbindungsname: Geben Sie einen aussagekräftigen Namen für die L2TP-over-IPsec-Verbindung ein, sodass iOS-Benutzer die Verbindung identifizieren können, die sie im Begriff sind, aufzubauen.Der Name Ihrer Firma gefolgt vom Protokoll L2TP-over-IPsec ist voreingestellt.

Hinweis – *Der Verbindungsname* muss für alle iOS-Verbindungseinstellungen (PPTP, L2TP-over-IPsec, Cisco VPN Client) eindeutig sein.

Hostnamen übergehen: Im Falle, dass der Systemhostname vom Client nicht öffentlich aufgelöst werden kann, können Sie hier einen Server-Hostnamen eingeben, der die interne Präferenz übergeht, bei der der *DynDNS-Hostname* dem *System-DNS-Hostnamen* vorgezogen wird.

Um die automatische iOS-Geräte-Konfiguration zu deaktivieren, klicken Sie auf den Schieberegler.

Der Schieberegler wird grau.

16.3.3 Fehlersuche

IKE-Fehlersuche

Im Abschnitt *IKE-Fehlersuche* können Sie die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest, für welche Arten von IKE-Nachrichten oder -Kommunikation zusätzliche Informationen in das Fehlerprotokoll geschrieben werden.

Hinweis – Der Abschnitt *IKE-Fehlersuche* ist für die Registerkarten *Fehlersuche* der Menüs *Site-to-Site VPN IPsec*, *Fernzugriff IPsec*, *L2TP über IPsec* und *Cisco VPN Client identisch*.

Die folgenden Flags können protokolliert werden:

- **Datenflusskontrolle:** Kontrollnachrichten zum IKE-Status
- **Ausgehende Pakete:** Inhalte von ausgehenden IKE-Nachrichten
- **Eingehende Pakete:** Inhalte von eingehenden IKE-Nachrichten
- **Kernel-Messaging:** Kommunikationsnachrichten mit dem Kernel
- **Hochverfügbarkeit:** Kommunikation mit anderen Hochverfügbarkeitsknoten

L2TP-Fehlersuche

Wenn die Option *Fehlersuche-Modus aktivieren* ausgewählt ist, enthält die Protokolldatei *IPsec-VPN* weitere Informationen zur Aushandlung von L2TP- oder PPP-Verbindungen.

16.4 IPsec

IP Security (IPsec) ist ein Standard für die Sicherung von *Internet-Protocol-*(IP-)Kommunikationen durch Verschlüsselung und/oder Authentifizierung aller IP-Pakete.

Der IPsec-Standard kennt zwei Betriebsarten (Modi) und zwei Protokolle:

- Transportmodus (engl. Transport Mode)
- Tunnelmodus (engl. Tunnel Mode)
- *Authentication Header* (AH): Protokoll für Authentifizierung
- *Encapsulated Security Payload* (ESP): Protokoll für Verschlüsselung (und Authentifizierung)

Des Weiteren bietet IPsec Methoden für die manuelle und die automatische Verwaltung von *Sicherheitsverbindungen* (SAs, engl. Security Associations) sowie zur Schlüsselverteilung. Alle diese Merkmale wurden in einer *Domain of Interpretation* (DOI) zusammengefasst.

IPsec-Modi

IPsec kann entweder im Transportmodus oder im Tunnelmodus arbeiten. Eine Host-zu-Host-Verbindung kann grundsätzlich jeden Modus verwenden. Wenn es sich bei einem der beiden Tunnelendpunkte jedoch um eine Firewall handelt, muss der Tunnelmodus verwendet werden. Die IPsec-VPN-Verbindungen auf der UTM arbeiten immer im Tunnelmodus.

Im Transportmodus wird das zu bearbeitende IP-Paket nicht in ein anderes IP-Paket eingepackt. Der ursprüngliche IP-Header wird beibehalten und das übrige Paket wird entweder in

Klartext (AH) oder verschlüsselt (ESP) gesendet. Nun kann entweder das komplette Paket mit AH authentifiziert oder die Payload mit Hilfe von ESP verschlüsselt und authentifiziert werden. In beiden Fällen wird der Original-Header in Klartext über das WAN geschickt.

Im Tunnelmodus wird das komplette Paket – Header und Payload – in ein neues IP-Paket gekapselt. Ein IP-Header wird vorne an das IP-Paket angehängt, wobei die Zieladresse auf den empfangenden Tunnelendpunkt gesetzt wird. Die IP-Adressen des gekapselten Paketes bleiben unverändert. Das Originalpaket kann dann mit AH authentifiziert oder mit ESP authentifiziert und verschlüsselt werden.

IPsec-Protokolle

IPsec verwendet für die sichere Kommunikation auf IP-Ebene zwei Protokolle:

- **Authentication Header (AH):** Ein Protokoll für die Authentifizierung von Absendern eines Pakets sowie zur Überprüfung der Integrität des Paketinhalts.
- **Encapsulating Security Payload (ESP):** Ein Protokoll für die Verschlüsselung des gesamten Pakets sowie für die Authentifizierung seines Inhalts.

Das *Authentication-Header*-Protokoll (AH) überprüft die Authentizität und die Integrität des Paketinhalts. Des Weiteren überprüft es, ob die Sender- und Empfänger-IP-Adressen während der Übertragung geändert wurden. Die Authentifizierung des Pakets erfolgt anhand einer Prüfsumme, die mittels eines *Hash-based Message Authentication Codes* (HMAC) in Verbindung mit einem Schlüssel und einem Hash-Algorithmus berechnet wurde. Einer der folgenden Hash-Algorithmen wird verwendet:

- **Message Digest Version 5 (MD5):** Dieser Algorithmus erzeugt aus einer Nachricht mit beliebiger Länge eine 128-Bit-lange Prüfsumme. Diese Prüfsumme ist wie ein Fingerabdruck des Paketinhalts und ändert sich, wenn die Nachricht verändert wird. Dieser Hash-Wert wird manchmal auch als digitale Signatur oder als Message Digest bezeichnet.
- **Secure Hash (SHA-1):** Dieser Algorithmus erzeugt analog zum MD5 einen 160-Bit-langen Hash-Wert. SHA-1 ist aufgrund des längeren Schlüssels sicherer als MD5.

Der Aufwand, einen Hash-Wert mittels SHA-1 zu berechnen, ist im Vergleich zum MD5-Algorithmus etwas höher. Die Berechnungsgeschwindigkeit hängt natürlich von der Prozessorgeschwindigkeit und der Anzahl der IPsec-VPN-Verbindungen ab, die auf der Sophos UTM verwendet werden.

Das *Encapsulated-Security-Payload*-Protokoll (ESP) bietet zusätzlich zur Verschlüsselung auch die Möglichkeit, den Absender zu authentifizieren und den Paketinhalt zu verifizieren. Wenn ESP im Tunnelmodus verwendet wird, wird das komplette IP-Paket (Header und Payload) verschlüsselt. Zu diesem verschlüsselten Paket wird ein neuer unverschlüsselter IP- und ESP-Header hinzugefügt: Der neue IP-Header beinhaltet die Adresse des Empfänger-Gateways und die Adresse des Absender-Gateways. Diese IP-Adressen entsprechen denen des VPN-Tunnels.

Für ESP mit Verschlüsselung werden üblicherweise die folgenden Algorithmen verwendet:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Von diesen bietet AES den höchsten Sicherheitsstandard. Die effektiven Schlüssellängen, die mit AES verwendet werden können, sind 128, 192 oder 256 Bit. Sophos UTM unterstützt mehrere Verschlüsselungs-Algorithmen. Für die Authentifizierung kann der MD5- oder der SHA-1-Algorithmus verwendet werden.

NAT-Traversal (NAT-T)

NAT-Traversal ist ein Verfahren, um zwischen Hosts in TCP/IP-Netzwerken Verbindungen über NAT-Geräte aufzubauen. Dies wird erreicht, indem UDP-Verkapselung der ESP-Pakete genutzt wird, um IPsec-Tunnel über NAT-Geräte aufzubauen. Die UDP-Verkapselung wird nur verwendet, wenn zwischen den IPsec-Gegenstellen NAT gefunden wird; andernfalls werden normale ESP-Pakete verwendet.

Mit NAT-Traversal kann ein IPsec-Tunnel auch aufgebaut werden, wenn sich das Gateway oder ein Road Warrior hinter einem NAT-Router befindet. Wenn Sie diese Funktion nutzen wollen, müssen allerdings beide IPsec-Endpunkte NAT-Traversal unterstützen – das wird automatisch ausgehandelt. Zusätzlich muss auf dem NAT-Gerät der IPsec-Passthrough (IPsec-Durchreichung) ausgeschaltet sein, da dies NAT-Traversal beeinträchtigen kann.

Wenn Road Warriors NAT-Traversal verwenden wollen, muss ihr entsprechendes Benutzerobjekt im WebAdmin eine statische Fernzugriffs-IP-Adresse (RAS, engl. remote static IP address) besitzen (siehe auch *Statische Fernzugriffs-IP verwenden* auf der Seite Benutzer im WebAdmin).

Um zu verhindern, dass der Tunnel abgebaut wird, wenn keine Daten übermittelt werden, sendet NAT-Traversal standardmäßig in einem Intervall von 60 Sekunden ein Signal zur Auf-

rechterhaltung (engl. keep alive).Durch dieses Aufrechterhaltungssignal wird sichergestellt, dass der NAT-Router die Statusinformation der Sitzung behält, damit der Tunnel offen bleibt.

TOS

Type-of-Service-Bits (TOS) sind einige Vier-Bit-Flags im IP-Header. Die Bits werden *Type-of-Service*-Bits genannt, da sie es der übertragenden Anwendung ermöglichen, dem Netzwerk mitzuteilen, welche Art von Dienstqualität benötigt wird.

Bei der IPsec-Implementierung von Sophos UTM wird der TOS-Wert immer kopiert.

16.4.1 Verbindungen

Auf der Registerkarte *IPsec* > *Verbindungen* können Sie IPsec-Verbindungen anlegen und bearbeiten.

Um eine IPsec-Verbindung zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue IPsec-Fernzugriffsregel*.**
   Das Dialogfeld *IPsec-Fernzugriffsregel hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Verbindung ein.

   Schnittstelle: Wählen Sie den Namen der Schnittstelle aus, die als lokaler Endpoint für den IPsec-Tunnel dienen soll.

   Lokale Netzwerke: Wählen Sie die lokalen Netzwerke aus, die über den VPN-Tunnel erreichbar sein sollen, oder fügen Sie sie hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

   Virtueller IP-Pool: Dies ist der IP-Adressenpool, aus dem die Clients eine IP-Adresse erhalten, falls sie keine statische IP-Adresse haben. Der Standardpool ist *VPN Pool (IPsec)*, der den privaten IP-Bereich `10.242.4.0/24` umfasst. Sie können jedoch auch einen anderen IP-Adressenpool auswählen. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer* > *Netzwerkdefinitionen* > *Netzwerkdefinitionen* erläutert.

Richtlinie: Wählen Sie die IPsec-Richtlinie für diese IPsec-Verbindung aus.IPsec-Richtlinien können auf der Registerkarte *Fernzugriff > IPsec > Richtlinien* definiert werden.

Auth.-Methode: Wählen Sie die Authentifizierungsmethode für diese Definition des entfernten Gateways aus.Die folgenden Typen sind verfügbar:

- **Verteilter Schlüssel:** Authentifizierung mit *Verteilten Schlüsseln* (PSK, engl. Preshared Keys) verwendet geheime Kennwörter als Schlüssel. Diese Kennwörter müssen an die Endpunkte verteilt werden, bevor eine Verbindung aufgebaut wird. Wenn ein neuer VPN-Tunnel aufgebaut ist, überprüft jede Seite, ob die andere Seite das geheime Kennwort kennt. Die Sicherheit der PSKs hängt von der Qualität der verwendeten Kennwörter ab: Normale Wörter und Ausdrücke fallen schnell Wörterbuchangriffen zum Opfer. Permanente oder längerfristige IPsec-Verbindungen sollten stattdessen Zertifikate verwenden.
- **X.509-Zertifikat:** Das X.509-Zertifikat basiert auf öffentlichen Schlüsseln und privaten Schlüsseln. Ein X.509-Zertifikat enthält den öffentlichen Schlüssel zusammen mit zusätzlichen Informationen über den Besitzer des Schlüssels. Solche Zertifikate sind von einer CA (*Zertifizierungsstelle*, engl. Certificate Authority) signiert und ausgestellt, der der Besitzer vertraut. Wenn Sie diese Authentifizierungsmethode wählen, geben Sie die Benutzer an, die diese IPsec-Verbindung benutzen dürfen. Wenn Sie die Option *Automatische Firewallregeln* nicht auswählen, müssen Sie entsprechende Firewallregeln manuell im Menü *Network Protection* anlegen.

  Hinweis – Auf das Benutzerportal kann nur von Benutzern zugegriffen werden, die im Feld *Zugelassene Benutzer* ausgewählt sind und für die eine Benutzerdefinition auf der UTM existiert.Autorisierte Benutzer, die sich erfolgreich am Benutzerportal angemeldet haben, finden den *Sophos-IPsec-Client* (SIC), dessen Konfigurationsdatei, die `PKCS#12-Datei` sowie einen Link zur Installationsanleitung vor, die in der Sophos-Knowledgebase zur Verfügung steht.

- **CA-DN-Vergleich:** Bei dieser Authentifizierungsmethode (engl. CA DN Match) wird ein Vergleich des *Distinguished Name* (DN) der CA-Zertifikate durchgeführt, um die Schlüssel der VPN-Endpoints zu verifizieren. Wenn Sie diese Authentifizierungsmethode wählen, wählen Sie eine *CA* und eine *DN-Maske*, die zu den DNs der Fernzugriff-Clients passt. Wählen Sie danach einen *Peer-Subnetzbereich* aus oder fügen Sie einen hinzu. Clients ist es nur gestattet, sich zu verbinden, wenn die DN-Maske zu derjenigen in ihrem Zertifikat passt.

XAUTH aktivieren (optional): XAUTH, erweiterte Authentifizierung (engl. extended authentication), sollte aktiviert werden, um von Benutzern eine Authentifizierung gegen konfigurierte Backends zu verlangen.

Automatische Firewallregeln (optional): Diese Funktion steht nur bei der Authentifizierungsmethode *X.509-Zertifikat* zur Verfügung. Wählen Sie diese Option, um automatisch Firewallregeln hinzuzufügen, die Datenverkehr für diese Verbindung zulassen. Die Regeln werden hinzugefügt, sobald die Verbindung aktiviert wird und sie werden entfernt, wenn die Verbindung deaktiviert wird.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Fernzugriffsregel wird in der Liste *Verbindungen* angezeigt.

Um eine Fernzugriffsregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

16.4.2 Richtlinien

Auf der Registerkarte *Fernzugriff > IPsec > Richtlinien* können Sie die Parameter für IPsec-Verbindungen definieren und in einer Richtlinie (Policy) zusammenfassen. Eine IPsec-Richtlinie legt die Internet-Schlüsselaustausch-Methode (IKE, Internet Key Exchange) und die IPsec-Antragsparameter für eine IPsec-Verbindung fest. Jede IPsec-Verbindung benötigt eine IPsec-Richtlinie.

Hinweis – Sophos UTM in IKE-Phase 1 wird nur der Hauptmodus unterstützt. Der aggressive Modus (engl. aggressive mode) wird nicht unterstützt.

Um eine IPsec-Richtlinie zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Richtlinie* auf *Neue IPsec-Richtlinie*.**
   Das Dialogfeld *IPsec-Richtlinie hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Richtlinie ein.

IKE-Verschlüsselungsalgorithmus: Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der IKE-Nachrichten verwendet wird. Die folgenden Algorithmen werden unterstützt:

- *DES* (56 Bit)
- *3DES* (168 Bit)
- *AES 128* (128 Bit)
- *AES 192* (192 Bit)
- *AES 256* (256 Bit)
- *Blowfish* (128 Bit)
- *Twofish* (128 Bit)
- *Serpent* (128 Bit)

Sicherheitshinweis – Es wird dringend davon abgeraten, DES zu verwenden, da dieser schwache Algorithmus eine potentielle Schwachstelle darstellt.

IKE-Authentifizierungsalgorithmus: Der Authentifizierungsalgorithmus legt fest, welcher Algorithmus verwendet wird, um die Intaktheit der IKE-Nachrichten zu prüfen. Die folgenden Algorithmen werden unterstützt:

- *MD5* (128 Bit)
- *SHA1* (160 Bit)
- *SHA2 256* (256 Bit)
- *SHA2 384* (384 Bit)
- *SHA2 512* (512 Bit)

IKE-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IKE-SA (Security Association, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 28800 Sekunden (8 Std.). Als Standardwert sind 7800 Sekunden voreingestellt.

IKE-DH-Gruppe: Während der Aushandlung einer Verbindung gleichen die beiden Gegenstellen auch die aktuellen Schlüssel für die Datenverschlüsselung ab. Für die Generierung des Sitzungsschlüssels (session key) nutzt IKE den *Diffie-Hellman*-(DH-)

Algorithmus. Dieser Algorithmus generiert den Schlüssel per Zufallsprinzip basierend auf sogenannten Pool Bits. Die IKE-Gruppe gibt hauptsächlich Aufschluss über die Anzahl der Pool Bits. Je mehr Pool Bits, umso länger ist die zufällige Zahlenkette – je größer die Zahlenkette, umso schwerer kann der Diffie-Hellman-Algorithmus geknackt werden. Folglich bedeuten mehr Pool Bits höhere Sicherheit, was allerdings auch bedeutet, dass mehr CPU-Leistung für die Generierung benötigt wird. Momentan werden die folgenden Diffie-Hellman-Gruppen unterstützt:

- *Gruppe 1: MODP 768*
- *Gruppe 2: MODP 1024*
- *Gruppe 5: MODP 1536*
- *Gruppe 14: MODP 2048*
- *Gruppe 15: MODP 3072*
- *Gruppe 16: MODP 4096*

Sicherheitshinweis – Gruppe 1 (MODP 768) wird allgemein als sehr schwach eingestuft und wird hier nur aus Kompatibilitätsgründen unterstützt. Wir raten dringend davon ab, sie zu verwenden, da sie eine potenzielle Schwachstelle darstellt.

IPsec-Verschlüsselungsalgorithmus: Die gleichen Verschlüsselungsalgorithmen wie für IKE.Zusätzlich gibt es die folgenden Einträge:

- *Keine Verschlüsselung (null)*
- *AES 128 CTR* (128 Bit)
- *AES 192 CTR* (192 Bit)
- *AES 256 CTR* (256 Bit)
- *AES 128 GCM (96 Bit)*
- *AES 192 GCM (96 Bit)*
- *AES 256 GCM (96 Bit)*
- *AES 128 GCM (128 Bit)*
- *AES 192 GCM (128 Bit)*
- *AES 256 GCM (128 Bit)*

> **Sicherheitshinweis –** Wir raten dringend davon ab, keine Verschlüsselung oder DES zu verwenden, da beides eine potenzielle Schwachstelle darstellt.

IPsec-Authentifizierungsalgorithmus: Die gleichen Authentifizierungsalgorithmen wie für IKE.Zusätzlich werden noch folgende Algorithmen unterstützt:

- *SHA2 256* (96 Bit)
- *SHA2 384* (96 Bit)
- *SHA2 512* (96 Bit)

Diese sind für die Kompatibilität mit Tunnelendpunkten verfügbar, die nicht RFC 4868 entsprechen, beispielsweise frühere UTM-Versionen (d. h. ASG-Versionen) als V8, und deshalb keine abgeschnittenen Prüfsummen länger als 96 Bit unterstützen.

IPsec-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IPsec-SA (Security Association, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 86400 Sekunden (1 Tag). Als Standardwert sind 3600 Sekunden voreingestellt.

IPsec-PFS-Gruppe: *Perfect Forward Secrecy* (PFS) ist eine Eigenschaft von Verschlüsselungsverfahren, die sicherstellt, dass aus einem geknackten Schlüssel nicht auf vorhergehende oder nachfolgende Sitzungsschlüssel einer Kommunikationsverbindung geschlossen werden kann. Damit PFS besteht, darf der zum Schutz der IPsec-SA-Verbindung genutzte Schlüssel nicht von demselben zufällig erzeugten Verschlüsselungsmaterial hergeleitet worden sein wie die Schlüssel für die IKE-SA-Verbindung. Daher initiiert PFS einen zweiten Diffie-Hellman-Schlüsselaustausch mit der Absicht, der ausgewählten DH-Gruppe für die IPsec-Verbindung einen neuen zufällig erzeugten Schlüssel zu übergeben. Es werden die gleichen DH-Gruppen wie bei IKE unterstützt.
Die Aktivierung von PFS wird als sicherer eingestuft, aber es benötigt auch mehr Zeit bei der Aushandlung. Es wird davon abgeraten, PFS auf langsamer Hardware einzusetzen.

> **Hinweis –** PFS ist nicht immer gänzlich kompatibel mit den verschiedenen Herstellern. Wenn Sie Probleme während der Aushandlung feststellen, schalten Sie diese Funktion aus.

Strikte Richtlinie: Wenn ein IPsec-Gateway eine Anfrage hinsichtlich eines Verschlüsselungsalgorithmus und der Verschlüsselungsstärke unternimmt, kann es vorkommen, dass das Gateway des Empfängers diese Anfrage akzeptiert, obwohl das nicht mit der entsprechenden IPsec-Richtlinie übereinstimmt. Wenn Sie diese Option wählen und der entfernte Endpunkt nicht exakt die von Ihnen festgelegten Parameter verwenden will, kommt keine IPsec-Verbindung zustande. Angenommen, die IPsec-Richtlinie Ihrer UTM verlangt AES-256-Verschlüsselung, wohingegen ein Road Warrior mit SSH-Sentinel sich mit AES-128 verbinden will – wenn die Option für die strikte Richtlinie aktiviert ist, wird die Verbindung abgewiesen.

> **Hinweis –** Die Komprimierungseinstellung wird durch Aktivierung der Option *Strikte Richtlinie* nicht erzwungen.

Komprimierung: Diese Option legt fest, ob IP-Pakete vor der Verschlüsselung mit dem *IP Payload Compression Protocol* (IPComp) komprimiert werden. IPComp reduziert die Größe von IP-Paketen, indem es sie komprimiert, um die allgemeine Kommunikationsleistung zwischen einem Paar von kommunizierenden Hosts oder Gateways zu erhöhen. Komprimierung ist standardmäßig ausgeschaltet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**
   Die neue Richtlinie wird in der Liste *Richtlinien* angezeigt.

Um eine Richtlinie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

16.4.3 Erweitert

Auf der Registerkarte *Fernzugriff* > *IPsec* > *Erweitert* können Sie die erweiterten Einstellungen für IPsec-VPN vornehmen.Abhängig von Ihrer bevorzugten Authentifizierungsmethode können Sie unter anderem das lokale Zertifikat (für X.509-Authentifizierung) und den lokalen RSA-Schlüssel (für RSA-Authentifizierung) festlegen. Diese Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

Lokales X.509-Zertifikat

Bei der X.509-Authentifizierung werden Zertifikate verwendet, um die öffentlichen Schlüssel der VPN-Endpunkte zu überprüfen. Wenn Sie diese Authentifizierungsmethode verwenden wollen, müssen Sie im Abschnitt *Lokales X.509-Zertifikat* ein lokales Zertifikat aus der Auswahlliste wählen. Das ausgewählte Zertifikat bzw. der Schlüssel wird anschließend dafür genutzt, das Gateway gegenüber Gegenstellen zu authentifizieren, falls X.509-Authentifizierung ausgewählt ist.

Sie können nur Zertifikate auswählen, für die auch der zugehörige private Schlüssel vorhanden ist, andere Zertifikate sind in der Auswahlliste nicht verfügbar.

Wenn keine Zertifikate zur Auswahl angezeigt werden, müssen Sie zunächst eines im Menü *Zertifikatverwaltung* hinzufügen, entweder indem Sie ein neues erzeugen oder indem Sie eines über die Hochladen-Funktion importieren.

Nachdem Sie das Zertifikat ausgewählt haben, geben Sie das Kennwort ein, mit dem der private Schlüssel geschützt ist. Während des Speichervorgangs wird das Kennwort verifiziert und eine Fehlermeldung angezeigt, falls das Kennwort nicht zum verschlüsselten Schlüssel passt.

Sobald ein aktiver Schlüssel oder ein Zertifikat ausgewählt ist, wird er/es im Abschnitt *Lokales X.509-Zertifikat* angezeigt.

Dead Peer Detection (DPD)

Dead Peer Detection verwenden: Die IPsec-Verbindung wird automatisch beendet, wenn das VPN-Gateway oder der Client auf der Gegenseite nicht erreichbar ist. Bei Verbindungen mit statischen Endpunkten wird der Tunnel nach einem Ausfall automatisch neu ausgehandelt. Für Verbindungen mit dynamischen Endpunkten wird für eine neue Aushandlung des Tunnels die Anfrage seitens der Gegenstelle benötigt. In der Regel ist diese Funktion betriebssicher und kann immer eingeschaltet bleiben. Die IPsec-Partner bestimmen automatisch, ob die Gegenstelle Dead Peer Detection unterstützt oder nicht, und verwenden den normalen Modus, falls nötig.

NAT-Traversal (NAT-T)

NAT-Traversal verwenden: Wählen Sie diese Option, um zu ermöglichen, dass IPsec-Verkehr Upstream-Systeme passieren kann, die *Network Address Translation* (NAT, dt. Netzwerkadressumsetzung) verwenden. Zusätzlich können Sie das Intervall für die Aufrechterhaltung (engl. keep-alive) für NAT-Traversal festlegen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

CRL-Handhabung

Es sind Situationen denkbar, in denen ein Zertifikataussteller noch während der Gültigkeitsdauer eines Zertifikats die darin gegebene Bestätigung für ungültig erklären möchte, z. B. weil zwischenzeitlich bekannt wurde, dass das Zertifikat vom Zertifikatnehmer unter Angabe falscher Daten (Name usw.) erschlichen wurde oder weil der zum zertifizierten öffentlichen Schlüssel gehörende private Schlüssel einem Angreifer in die Hände gefallen ist. Zu diesem Zweck werden sogenannte *Zertifikatsperrlisten* (CRLs, engl. Certificate Revocation Lists) verwendet. Diese enthalten üblicherweise die Seriennummern derjenigen Zertifikate einer Zertifizierungsinstanz, die für ungültig erklärt werden und deren regulärer Gültigkeitszeitraum noch nicht abgelaufen ist.
Nach Ablauf dieses Zeitraums besitzt das Zertifikat in jedem Fall keine Gültigkeit mehr und muss daher auch nicht weiter auf der Zertifikatsperrliste geführt werden.

Automatische Abholung: Mit dieser Funktion wird die CRL automatisch über die URL abgeholt, die im Partnerzertifikat angegeben ist, via HTTP, anonymes FTP (Anonymous FTP) oder LDAP Version 3. Die CRL kann auf Anfrage heruntergeladen, abgespeichert und aktualisiert werden, sobald der Gültigkeitszeitraum abgelaufen ist. Wenn Sie diese Funktion nutzen (jedoch nicht über Port 80 oder 443), achten Sie darauf, dass die Firewallregeln so gesetzt sind, dass auf den CRL-Distributionsserver zugegriffen werden kann.

Strikte Richtlinie: Wenn Sie diese Option auswählen, werden alle Partnerzertifikate ohne eine zugehörige CRL zurückgewiesen.

Probing von verteilten Schlüsseln

Für IPsec-Verbindungen, die im Nur-Antworten-Modus (engl. respond-only) arbeiten, können Sie festlegen, dass mehrere verteilte Schlüssel (PSK, engl. preshared keys) für jede IPsec-Verbindung zugelassen sind.

Probing von verteilten Schlüsseln: Markieren Sie das Auswahlkästchen, um die Funktion zu aktivieren. Diese Option betrifft L2TP-über-IPsec-, IPsec-Fernzugriff- und IPsec-Site-to-Site-Verbindungen.

16.4.4 Fehlersuche

IKE-Fehlersuche

Im Abschnitt *IKE-Fehlersuche* können Sie die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest, für welche Arten von IKE-Nachrichten oder -Kommunikation

zusätzliche Informationen in das Fehlerprotokoll geschrieben werden.

Hinweis – Der Abschnitt *IKE-Fehlersuche* ist für die Registerkarten *Fehlersuche* der Menüs *Site-to-Site VPN IPsec*, *Fernzugriff IPsec*, *L2TP über IPsec* und *Cisco VPN Client identisch*.

Die folgenden Flags können protokolliert werden:

- **Datenflusskontrolle:** Kontrollnachrichten zum IKE-Status
- **Ausgehende Pakete:** Inhalte von ausgehenden IKE-Nachrichten
- **Eingehende Pakete:** Inhalte von eingehenden IKE-Nachrichten
- **Kernel-Messaging:** Kommunikationsnachrichten mit dem Kernel
- **Hochverfügbarkeit:** Kommunikation mit anderen Hochverfügbarkeitsknoten

16.5 HTML5-VPN-Portal

Das HTML5-VPN-Portal ermöglicht Benutzern in externen Netzwerken den Zugriff auf interne Ressourcen über vorkonfigurierte Verbindungstypen und einen normalen Webbrowser ohne zusätzliche Plug-ins. Der Benutzer meldet sich dafür am Benutzerportal von UTM an. Auf der Registerkarte *HTML5-VPN-Portal* wird eine Liste aller Verbindungen angezeigt, die für diesen Benutzer definiert sind. Wenn der Benutzer auf die Schaltfläche *Verbinden* klickt, wird eine Verbindung zur festgelegten internen Ressource hergestellt. Als Administrator müssen Sie diese Verbindungen vorher erstellen und die zugelassenen Benutzer, den Verbindungstyp und andere Einstellungen festlegen. Der Zugriff auf interne Ressourcen kann über verschiedene Verbindungstypen erfolgen: Remote Desktop Protocol (RDP) oder Virtual Network Computing (VNC) für den Zugriff auf entfernte Computer, ein Browser für Webanwendungen (HTTP/HTTPS) oder Telnet/Secure Shell (SSH) für Terminal-Sitzungen. Über das HTML5-VPN-Portal können jedoch keine Inhalte, z. B. über HTTP, auf den lokalen Rechner des Benutzers heruntergeladen werden.

Mit dieser Funktion können Sie mehreren Benutzern Zugriff auf interne Ressourcen geben, auch wenn diese von sich aus keinen Mehrbenutzerzugriff unterstützen (z. B. Netzwerkhardware wie Switches). Auch lässt sich damit der Zugriff auf einen bestimmten Dienst beschränken, anstatt Vollzugriff auf ganze Systeme oder Netzwerke zu gewähren.

Beispiele:

- Geben Sie einem Telekommunikationsanbieter beschränkten Zugriff, damit er Ihre Telefoninfrastruktur warten kann.
- Erlauben Sie den Zugriff auf eine bestimmte interne Website, z. B. das Intranet.

Hinweis – Der Browser des Benutzers muss HTML5 unterstützen. Die folgenden Browser unterstützen die HTML5-VPN-Funktion: Firefox ab Version 6.0, Internet Explorer ab Version 10, Chrome, Safari ab Version 5 (nicht beim Betriebssystem Windows).

16.5.1 Allgemein

Auf der Registerkarte *Fernzugriff > HTML5-VPN-Portal > Allgemein* können Sie das HTML5-VPN-Portal einschalten und die VPN-Portal-Verbindungen verwalten. Beachten Sie, dass die Zahl der Verbindungen auf 100 begrenzt ist. Zugelassene Benutzer können auf der Registerkarte *HTML5-VPN-Portal* im Benutzerportal auf die für sie freigegebenen Verbindungen zugreifen.

Um das HTML5-VPN-Portal zu aktivieren und eine neue HTML5-VPN-Verbindung zu erstellen, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie das HTML5-VPN-Portal.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird grün und die Elemente auf der Seite können bearbeitet werden. Jetzt können zugelassene Benutzer alle vorhandenen, für sie freigegebenen Verbindungen im Benutzerportal sehen.

2. **Klicken Sie auf die Schaltfläche *Neue HTML5-VPN-Portal-Verbindung*.**
   Das Dialogfeld *HTML5-VPN-Portal-Verbindung hinzufügen* wird geöffnet.

3. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für diese Verbindung ein.

   Verbindungstyp: Wählen Sie den Verbindungstyp aus. Je nachdem, welchen Verbindungstyp Sie auswählen, werden unterschiedliche Parameter angezeigt. Die folgenden Typen sind verfügbar:

   - **Remotedesktop:** Fernzugriff über Remote Desktop Protocol (RDP), z. B. für eine Remotedesktopsitzung auf einem Windows-Host.
   - **Webapp (HTTP):** Browserbasierter Zugriff auf Webanwendungen über HTTP.

- **Webapp (HTTPS):** Browserbasierter Zugriff auf Webanwendungen über HTTPS.

  Hinweis – Die für die HTTP/HTTPS-Verbindung verwendete URL setzt sich aus den Verbindungsoptionen *Ziel*, *Port* und *Pfad* zusammen. Die Webanwendung muss mit Mozilla Firefox (ab Version 6.0) kompatibel sein.

- **Telnet:** Terminalzugriff über das Telnet-Protokoll, z. B. für den Zugriff auf einen Switch oder einen Drucker.
- **SSH:** Terminalzugriff über SSH.
- **VNC:** Fernzugriff über Virtual Network Computing (VNC), z. B. für eine Remotedesktopverbindung mit einem Linux/Unix-Host.

  Hinweis – Im Moment wird nur die klassische VNC-Authentifizierung (nur Kennwort) unterstützt. Stellen Sie sicher, dass Ihr Server entsprechend eingerichtet ist.

Ziel: Wählen Sie hier den Host aus, mit dem sich zugelassene Benutzer verbinden dürfen, oder fügen Sie ihn hinzu. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

Hinweis – Wenn der ausgewählte Zielhost ein selbstsigniertes Zertifikat bereitstellt, muss der CN (Common Name) des Zertifikats mit dem Namen Ihres Zielhosts übereinstimmen. Andernfalls wird dem Benutzer im Portal-Browser ein Warnhinweis angezeigt. Wenn Sie zum Beispiel den DNS-Host *www.meinedomaene.de* verwenden, muss dieser Name im selbstsignierten Zertifikat enthalten sein. Wenn Sie anstelle eines DNS-Hosts einen Host verwenden, muss das selbstsignierte Zertifikat die IP-Adresse des Hosts als *Subject Alternative Name* enthalten.

Pfad (nur bei den *Webapp*-Verbindungstypen): Geben Sie hier den Pfad ein, mit dem sich zugelassene Benutzer verbinden dürfen.

Benutzername (nur beim Verbindungstyp *SSH*): Geben Sie den Benutzernamen ein, den der Benutzer für die Verbindung verwenden soll.

Automatisch anmelden/Automatisch anmelden (einfache Auth.): Wenn aktiviert, können sich Benutzer ohne Kenntnis der Authentifizierungsdaten anmelden. In diesem Fall müssen Sie die Authentifizierungsdaten bereitstellen. Je nach Verbindungstyp werden unterschiedliche Optionen angezeigt:

- **Benutzername:** Geben Sie den Benutzernamen ein, den Benutzer für die Verbindung verwenden sollen.
- **Kennwort:** Geben Sie das Kennwort ein, das Benutzer für die Verbindung verwenden sollen.

> **Hinweis –** Wenn Sie den Verbindungstyp *Telnet* verwenden, funktioniert die automatische Anmeldung aus Sicherheitsgründen nur dann, wenn die Länge des Banners, das vom Telnet-Server gesendet wird, 4.096 Zeichen (inklusive Kennwort-Aufforderung) nicht überschreitet. Wenn das Banner länger ist, schlägt die Anmeldung fehl. Reduzieren Sie in diesem Fall die Bannerlänge oder schalten Sie auf manuelle Anmeldung um.

- **Authentifizierungsmethode** (nur beim Verbindungstyp *SSH*): Wählen Sie die SSH-Authentifizierungsmethode. Sie können entweder das *Kennwort* für den ausgewählten Benutzernamen oder den *Privaten SSH-Schlüssel* für die SSH-Verbindung angeben.

SSL-Hostzertifikat (nur beim Verbindungstyp *HTTPS*): Fügen Sie das SSL-Host-Sicherheitszertifikat hinzu, mit dem der Zielhost identifiziert wird.

- **SSL-Zertifikat:** Klicken Sie auf die Schaltfläche *Abrufen*, um das Zertifikat automatisch zum ausgewählten Zielhost hinzuzufügen.

Öffentlicher Host-Schlüssel (nur beim Verbindungstyp *SSH*): Fügen Sie den öffentlichen Schlüssel des SSH-Hosts hinzu.

- **Öffentlicher SSH-Schlüssel:** Klicken Sie auf die Schaltfläche *Abrufen*, um den öffentlichen SSH-Schlüssel des ausgewählten Zielhosts automatisch abzurufen.

Zugelassene Benutzer (Benutzerportal): Wählen Sie die Benutzer oder Gruppen aus, die Zugriff auf die VPN-Portal-Verbindung haben sollen, oder fügen Sie die neuen Benutzer hinzu. Standardmäßig kann eine Verbindung immer nur von einem Benutzer gleichzeitig verwendet werden. Wenn Sie möchten, dass eine Verbindung von mehreren Benutzern gleichzeitig verwendet werden kann, aktivieren Sie das Auswahlkästchen

Gemeinsame Sitzung im Abschnitt *Erweitert*. Das Hinzufügen eines Benutzers wird auf der Seite *Definitionen & Benutzer* > *Benutzer & Gruppen* > *Benutzer* erläutert.

> **Hinweis –** Wenn Sie eine Gruppe mit Backend-Mitgliedschaft hinzufügen, muss diese Gruppe für das Benutzerportal zugelassen sein. Auf der Registerkarte *Verwaltung* > *Benutzerportal* > *Allgemein* wählen Sie dafür entweder *Alle Benutzer zulassen* oder *Nur bestimmte Benutzer zulassen* und fügen Sie die fragliche Gruppe explizit hinzu. Wenn Sie nur einzelne Gruppenmitglieder für das Benutzerportal zulassen, erhalten diese keinen Zugriff auf die Verbindungen, die für die Gruppe zugelassen sind.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

4. **Optional können Sie die folgenden erweiterten Einstellungen vornehmen:**

   Port: Geben Sie eine Portnummer für die Verbindung ein. Standardmäßig ist dies der Standardport des ausgewählten Verbindungstyps.

   Protokollsicherheit (nur beim Verbindungstyp *Remotedesktop*): Wählen Sie das Sicherheitsprotokoll für die Remotedesktopsitzung. Sie können zwischen RDP, TLS und NLA (Network Level Authentication) wählen. Ihre Einstellung muss mit der auf dem Server übereinstimmen. Für NLA müssen Sie oben *Automatisch anmelden* auswählen.

   Gemeinsame Sitzung: Wählen Sie diese Option, damit eine Verbindung von mehreren Benutzern gleichzeitig verwendet werden kann. Den Benutzern wird derselbe Bildschirm angezeigt.

   Externe Ressourcen erlauben (nur bei den Verbindungstypen *Webapp (HTTP/S)*): Geben Sie zusätzliche Ressourcen an, auf die über diese Verbindung zugegriffen werden darf. Dies ist beispielsweise nützlich, wenn Bilder oder andere Ressourcen auf einem anderen Server gespeichert sind als die Webseite selbst. Für die ausgewählten Hosts oder Netzwerkbereiche sind die Ports 80 und 443 erlaubt.

5. **Klicken Sie auf *Speichern*.**
   Die neue Verbindung wird in der Liste *Verbindungen* angezeigt.

6. **Aktivieren Sie die Verbindung.**
   Klicken Sie auf den Schieberegler, um die Verbindung zu aktivieren.

   Die Verbindung kann jetzt von den zugelassenen Benutzern verwendet werden. Sie finden sie auf der Registerkarte *HTML5-VPN-Portal* des Benutzerportals.

Um eine Verbindung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

16.6 Cisco VPN Client

Sophos UTMunterstützt IPsec-Fernzugriff über Cisco VPN Client. Der Cisco VPN Client ist ein ausführbares Programm von Cisco Systems, das es ermöglicht, entfernte Computer auf sichere Weise mit einem virtuellen privaten Netzwerk (VPN, *Virtual Private Network*) zu verbinden.

16.6.1 Allgemein

Auf der Registerkarte *Fernzugriff* > *Cisco VPN Client* > *Allgemein* können Sie die grundlegenden Optionen für den Fernzugriff über Cisco VPN Client konfigurieren.

Um die Sophos UTM so zu konfigurieren, dass Cisco-VPN-Client-Verbindungen zulässig sind, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Cisco VPN Client auf der Registerkarte *Allgemein*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Servereinstellungen* kann bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Schnittstelle: Wählen Sie eine Schnittstelle, die für Cisco-VPN-Client-Verbindungen verwendet werden soll.

   Serverzertifikat: Wählen Sie das Zertifikat, mit dem sich der Server gegenüber dem Client identifizieren soll.

   Pool-Netzwerk: Wählen Sie einen Netzwerk-Pool, dessen virtuelle Netzwerkadressen den Clients zugewiesen werden sollen, wenn sie sich verbinden. *VPN Pool (Cisco)* ist vorausgewählt.

   Benutzer und Gruppen: Wählen Sie Benutzer und/oder Gruppen, die sich mit UTM über Cisco VPN Client verbinden dürfen. Es ist jedoch nicht möglich, Backend-Mitgliedschaftsgruppen in das Feld zu ziehen, weil zum Zeitpunkt der IPsec-Konfiguration ein Benutzerzertifikat benötigt wird. Dieses Zertifikat wird aber nur erzeugt, wenn sich ein Benutzer zum ersten Mal erfolgreich angemeldet hat.

Lokale Netzwerke: Wählen Sie die lokalen Netzwerke aus, die über den VPN-Tunnel erreichbar sein sollen.

Automatische Firewallregeln (optional): Wählen Sie diese Option, um automatisch Firewallregeln hinzuzufügen, die Datenverkehr für diese Verbindung zulassen. Die Regeln werden hinzugefügt, sobald die Verbindung aktiviert wird und sie werden entfernt, wenn die Verbindung deaktiviert wird.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Live-Protokoll

Verwenden Sie das Live-Protokoll, um die Verbindungs-Protokolleinträge des IPsec-IKE-Daemon-Protokolls zu verfolgen. Es zeigt Informationen zum Aufbau, zur Aufrechterhaltung und zur Beendigung von Verbindungen an.

16.6.2 iOS-Geräte

Sie können ermöglichen, dass Benutzern von iOS-Geräten eine automatische Cisco-IPsec-Konfiguration im Benutzerportal angeboten wird.

Allerdings werden nur Benutzer, die im Feld *Benutzer und Gruppen* auf der Registerkarte *Allgemein* aufgeführt sind, die Konfigurationsdateien auf ihrer Benutzerportal-Seite finden. Der iOS-Geräte-Status ist standardmäßig aktiviert.

Verbindungsname: Geben Sie einen aussagekräftigen Namen für die Cisco IPsec-Verbindung ein, sodass iOS-Benutzer die Verbindung identifizieren können, die sie im Begriff sind, aufzubauen.Der Name Ihrer Firma gefolgt vom Protokoll Cisco IPsec ist voreingestellt.

Hinweis – *Der Verbindungsname* muss für alle iOS-Verbindungseinstellungen (PPTP, L2TP-over-IPsec, Cisco VPN Client) eindeutig sein.

Hostnamen übergehen: Im Falle, dass der Systemhostname vom Client nicht öffentlich aufgelöst werden kann, können Sie hier einen Server-Hostnamen eingeben, der die interne Präferenz übergeht, bei der der *DynDNS-Hostname* dem *System-DNS-Hostnamen* vorgezogen wird.

VPN-Verbindung bei Bedarf aufbauen: Wählen Sie diese Option, um automatisch eine VPN-Verbindung aufzubauen, sobald es eine Übereinstimmung mit einem der Hostnamen oder einer der Domänen gibt.

- **Übereinstimmung mit Domäne oder Host:** Geben Sie die Domänen und Hostnamen ein, für die Sie bei Bedarf VPN-Verbindungen aufbauen wollen. Das könnte beispielsweise Ihr lokales Intranet sein.
- **Nur aufbauen, wenn DNS-Lookup fehlschlägt:** Standardmäßig wird die VPN-Verbindung nur aufgebaut, nachdem ein DNS-Lookup fehlgeschlagen ist. Ist die Option nicht ausgewählt, wird die VPN-Verbindung aufgebaut, unabhängig davon, ob der Hostname aufgelöst werden kann oder nicht.

Beachten Sie, dass iOS-Geräten, die sich verbinden, das Serverzertifikat gezeigt wird, das auf der Registerkarte *Allgemein* definiert ist. Das iOS-Gerät überprüft dann, ob die VPN-ID dieses Zertifikats mit dem Server-Hostnamen übereinstimmt, und lehnt die Verbindung ab, wenn es keine Übereinstimmung gibt. Wenn das Serverzertifikat einen *Distinguished Name* als VPN-ID verwendet, vergleicht das iOS-Gerät den Server-Hostnamen stattdessen mit dem Feld *Allgemeiner Name* (Common Name).Sie müssen sicherstellen, dass das Server-Zertifikat diese Bedingungen erfüllt.

Um die automatische iOS-Geräte-Konfiguration zu deaktivieren, klicken Sie auf den Schieberegler.

Der Schieberegler wird grau.

16.6.3 Fehlersuche

IKE-Fehlersuche

Im Abschnitt *IKE-Fehlersuche* können Sie die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest, für welche Arten von IKE-Nachrichten oder -Kommunikation zusätzliche Informationen in das Fehlerprotokoll geschrieben werden.

Hinweis – Der Abschnitt *IKE-Fehlersuche* ist für die Registerkarten *Fehlersuche* der Menüs *Site-to-Site VPN IPsec*, *Fernzugriff IPsec*, *L2TP über IPsec* und *Cisco VPN Client identisch*.

Die folgenden Flags können protokolliert werden:

- **Datenflusskontrolle:** Kontrollnachrichten zum IKE-Status
- **Ausgehende Pakete:** Inhalte von ausgehenden IKE-Nachrichten
- **Eingehende Pakete:** Inhalte von eingehenden IKE-Nachrichten

- **Kernel-Messaging:** Kommunikationsnachrichten mit dem Kernel
- **Hochverfügbarkeit:** Kommunikation mit anderen Hochverfügbarkeitsknoten

16.7 Erweitert

Auf der Seite *Fernzugriff > Erweitert* können Sie die erweiterten Einstellungen für die Fernzugriff-Clients durchführen. Die IP-Adressen der DNS- und WINS-Server, die Sie hier angeben, werden für die Nutzung durch Fernzugriff-Clients während des Verbindungsaufbaus mit dem Gateway zur Verfügung gestellt, wodurch eine vollständige Namensauflösung für Ihre Domäne gewährleistet wird.

DNS-Server: Sie können bis zu zwei DNS-Server für Ihr Unternehmen definieren.

WINS-Server: Sie können bis zu zwei WINS-Server für Ihr Unternehmen definieren. *Windows Internet Naming Service* (WINS, dt. Windows Internet Namensdienst) ist Microsofts Implementierung des *NetBIOS Name Servers* (NBNS) für Windows-Betriebssysteme. Im Prinzip führt WINS für NetBIOS-Namen das durch, was DNS für Domänennamen durchführt: einen zentralen Abgleich zwischen Hostnamen und IP-Adressen.

Domänenname: Tragen Sie den *Fully Qualified Domain Name* (FQDN) Ihres Unternehmens ein. Der Fully Qualified Domain Name ist ein eindeutiger Domänenname, der in einer DNS-Baumstruktur die absolute Position des Knotens spezifiziert, z. B. `intranet.beispiel.de`.

> **Hinweis –** Bei PPTP und L2TP über IPsec kann der Domänenname *nicht* automatisch verteilt werden – er muss auf dem Client manuell konfiguriert werden.
> Bei iOS-Geräten, die *Cisco VPN Client* verwenden, wird der oben angegebene DNS-Server nur dazu verwendet, Hosts aufzulösen, die zu der definierten Domäne gehören.

16.8 Zertifikatverwaltung

Über das Menü *Fernzugriff > Zertifikatverwaltung*, das dieselben Konfigurationsoptionen enthält wie das Menü *Site-to-Site-VPN > Zertifikatverwaltung*, können Sie alle zertifikatbezogenen Vorgänge von Sophos UTM verwalten. Das beinhaltet unter anderem das Anlegen und Importieren von X.509-Zertifikaten sowie das Hochladen sogenannter *Zertifikatsperrlisten* (CRLs).

16.8.1 Zertifikate

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Zertifikate*.

16.8.2 Certificate Authority (Zertifizierungsstelle)

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *CA*.

16.8.3 Sperrlisten (CRLs)

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Sperrlisten (CRLs)*.

16.8.4 Erweitert

Gehen Sie zu *Site-to-Site-VPN* > *Zertifikatverwaltung* > *Erweitert*.

17 Protokolle & Berichte

Dieses Kapitel beschreibt die Protokoll- und Berichtsfunktionen von Sophos UTM.

Sophos UTMbietet umfangreiche Protokollfunktionen, indem es die verschiedenen Ereignisse betreffend den Schutz des Systems und des Netzwerks ununterbrochen aufzeichnet. Die detaillierten Protokollaufzeichnungen ermöglichen sowohl rückblickende als auch aktuelle Analysen der verschiedenen Netzwerkaktivitäten, durch die potenzielle Sicherheitsbedrohungen identifiziert oder aufkommende Probleme verhindert werden können.

Die Berichtsfunktion von Sophos UTM bietet System- und Netzwerkinformationen in Echtzeit. Dafür werden die Informationen aus den Protokolldateien gesammelt und in grafischer Form dargestellt.

Die Seite *Protokollpartitionsstatus* im WebAdmin zeigt den aktuellen Status der Protokollpartition auf Sophos UTM an, einschließlich Informationen über verbleibenden Speicherplatz und Zuwachsrate sowie ein Histogramm über die Nutzung der Protokollpartition in den letzten vier Wochen. Für die Berechnung der durchschnittlichen Zuwachsrate wird das aktuelle Datenvolumen durch die verstrichene Zeit dividiert – die Angaben sind daher zu Beginn etwas ungenau.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Protokollansicht
- Hardware
- Netzwerknutzung
- Network Protection
- Web Protection
- Email Protection
- Fernzugriff
- Webserver Protection
- Gesamtbericht
- Protokolleinstellungen
- Berichteinstellungen

Berichtsdaten-Diagramme

Sophos UTM zeigt Berichtsdaten als Linien- und Tortendiagramme an. Die Interaktivität dieser Diagramme ermöglicht einen feingranularen Zugang zu den Daten.

Liniendiagramme

Die Interaktion mit Liniendiagrammen ist einfach: Wenn Sie mit dem Mauszeiger über das Diagramm fahren, wird ein Punkt angezeigt, der Ihnen detaillierte Informationen zu diesem Teil des Diagramms liefert. Der Punkt haftet an der Linie des Diagramms. Er folgt den Bewegungen des Mauszeigers. Wenn ein Diagramm mehrere Linien hat, wechselt der Punkt zwischen ihnen, je nachdem, wohin Sie den Mauszeiger bewegen. Darüber hinaus ändert der Punkt seine Farbe in Abhängigkeit davon, auf welche Linie sich seine Informationen beziehen. Das ist besonders nützlich, wenn Linien eng nebeneinander liegen.

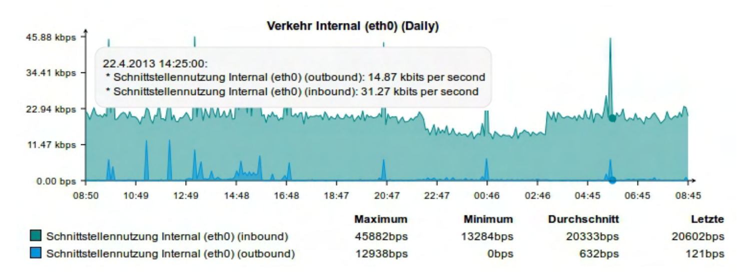


Bild 31 Berichte: Beispiel eines Liniendiagramms

Tortendiagramme

Ähnlich wie bei den Liniendiagrammen können Sie mit den Tortendiagrammen interagieren: Richten Sie den Mauszeiger auf ein Stück eines Tortendiagramms. Dieses Stück wird sofort vom Rest des Tortendiagramms hervorgehoben und der Tooltip zeigt Informationen zum hervorgehobenen Stück.

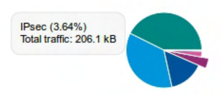


Bild 32 Berichte: Beispiel eines Tortendiagramms

17.1 Protokollansicht

Im Menü *Protokolle & Berichte* > *Protokollansicht* können die verschiedenen Protokolldateien angesehen und durchsucht werden.

17.1.1 Heutige Protokolldateien

Auf der Registerkarte *Protokolle & Berichte* > *Protokollansicht* > *Heutige Protokolldateien* können Sie auf alle aktuellen Protokolldateien zugreifen.

Diese Registerkarte bietet außerdem einige Aktionen, die auf alle Protokolldateien angewendet werden können. Die folgenden Aktionen sind möglich:

- **Live-Protokoll:** Ein Klick auf diese Schaltfläche öffnet ein neues Fenster, in dem Sie das Protokoll in Echtzeit mitverfolgen können. Neue Zeilen werden der Protokolldatei in Echtzeit hinzugefügt. Wenn Sie *Autoscroll* auswählen, läuft der Text im Fenster mit, sodass immer die aktuellsten Einträge angezeigt werden. Des Weiteren können Sie mit der Filterfunktion die Anzeige neuer Protokolleinträge einschränken, sodass nur jene Einträge angezeigt werden, die mit dem Ausdruck im Filter übereinstimmen.
- **Anschauen:** Ein Pop-Up-Fenster wird geöffnet, in dem der aktuelle Stand der Protokolldatei angezeigt wird.
- **Löschen:** Löscht den Inhalt der Protokolldatei.

Mit der Auswahlliste unterhalb der Tabelle können Sie vorher ausgewählte Protokolldateien entweder als `zip`-Datei herunterladen oder den Inhalt der Dateien auf einmal löschen.

17.1.2 Archivierte Protokolldateien

Auf der Registerkarte *Protokolle & Berichte* > *Protokollansicht* > *Archivierte Protokolldateien* können Sie das Protokollarchiv verwalten. Alle Protokolldateien werden täglich archiviert. Um auf eine archivierte Protokolldatei zuzugreifen, wählen Sie das Teilsystem von Sophos UTM aus, für das die Protokolle erstellt werden, sowie ein Jahr und einen Monat.

Alle verfügbaren Protokolldateien, die Ihrer Auswahl entsprechen, werden in chronologischer Reihenfolge angezeigt. Sie können die archivierten Protokolldateien entweder aufrufen oder im `zip`-Format herunterladen.

Mit der Auswahlliste unterhalb der Tabelle können Sie vorher ausgewählte Protokolldateien entweder als `zip`-Datei herunterladen oder alle auf einmal löschen.

17.1.3 Protokolldateien durchsuchen

Auf der Registerkarte *Protokolle & Berichte > Protokollansicht > Protokolldateien durchsuchen* können Sie Ihre lokalen Protokolldateien nach bestimmten Zeiträumen durchsuchen. Wählen Sie zunächst eine Protokolldatei, die Sie durchsuchen wollen. Geben Sie dann einen Suchbegriff ein und wählen Sie einen Zeitraum. Wenn Sie *Benutzerdefinierter Zeitraum* unter *Zeitraum* auswählen, können Sie ein Start- und Enddatum angeben. Nachdem Sie auf *Suche starten* geklickt haben, wird ein neues Fenster geöffnet, in dem die Ergebnisse Ihrer Suche angezeigt werden. Je nach Browser kann es nötig sein, Pop-up-Fenster für WebAdmin zu erlauben.

Wenn Sie *Webfilter* oder *Endpoint Web Protection* aus der Liste der zum Durchsuchen ausgewählten Protokolldateien auswählen, sind drei weitere Filterkategorien verfügbar.Sie können nach einem spezifischen *Benutzer*, einer spezifischen *URL* und einer spezifischen *Aktion suchen.*

- **Benutzer:** Sucht in den Protokolldateien nach dem vollständigen Benutzernamen.
- **URL:** Sucht nach einem Teilausdruck einer URL.
- **Aktion:** Auswahlliste mit verschiedenen Aktionen.

Hinweis – Wenn Sie das *Kontrollkästchen* unter dem *Suchbegriff* auswählen, können Sie optional dieselbe Suche für *Webfilter* und *Endpoint Protection* gleichzeitig ausführen.

17.2 Hardware

Das Menü *Protokolle & Berichte > Hardware* bietet einen statistischen Überblick über die Verwendung der Hardware-Komponenten für unterschiedliche Zeiträume.

17.2.1 Täglich

Die Registerkarte *Hardware > Täglich* bietet umfangreiche statistische Informationen zu den folgenden Hardware-Komponenten für die letzten 24 Stunden:

- CPU-Auslastung
- Speichernutzung: Speicher- bzw. Swap-Auslastung
- Partitionsnutzung: Speicherplatzbelegung der verschiedenen Partitionen

CPU-Auslastung: Das Histogramm zeigt die aktuelle Auslastung des Prozessors in Prozent an.

Speicher-/Swap-Auslastung: Das Diagramm zeigt die Auslastung von Speicher und Swap in Prozent an. Die Swap-Auslastung hängt stark von Ihrer Systemkonfiguration ab. Die Aktivierung von Systemdiensten wie Intrusion Prevention oder den Proxy-Servern führt zu einer höheren Speicherauslastung. Wenn kein freier Hauptspeicher mehr zur Verfügung steht, erfolgt der Zugriff auf den virtuellen Speicher (Swap), wodurch sich die gesamte Leistungsfähigkeit des Systems verschlechtert. Die Nutzung von Swap sollte so gering wie möglich sein. Um das zu erreichen, sollten Sie den verfügbaren Hauptspeicher erhöhen.

Auslastung der Speicherpartition: Die Diagramme zeigen die Auslastung ausgewählter Partitionen in Prozent an, wobei jede Partition durch einen eigenen Graph dargestellt wird:

- **Root:** Die Root-Partition ist die Partition, in der sich das Root-Verzeichnis von Sophos UTM befindet. Hier werden auch die Aktualisierungspakete und Backups gespeichert.
- **Protokollieren:** Die Protokollpartition ist die Partition, in der Protokolldateien und Berichtsdaten gespeichert werden. Wenn auf dieser Partition der freie Speicherplatz zur Neige geht, passen Sie unter *Protokolle & Berichte* > *Protokolleinstellungen* > *Lokale Protokollierung* die Einstellungen an.
- **Speicher:** Die Speicherpartition ist die Partition, in der Proxy-Dienste ihre Daten abspeichern, z. B. Bilder für den Webfilter, Meldungen für den SMTP-Proxy, E-Mails in Quarantäne usw. Darüber hinaus befinden sich hier die Datenbank, temporäre Daten und Konfigurationsdateien.

17.2.2 Wöchentlich

Die Registerkarte *Hardware* > *Wöchentlich* bietet umfangreiche statistische Informationen zu ausgewählten Hardware-Komponenten für die letzten sieben Tage. Die Histogramme werden unter *Täglich* beschrieben.

17.2.3 Monatlich

Die Registerkarte *Hardware* > *Monatlich* bietet umfangreiche statistische Informationen zu ausgewählten Hardware-Komponenten für die letzten vier Wochen. Die Histogramme werden unter *Täglich* beschrieben.

17.2.4 Jährlich

Die Registerkarte *Hardware* > *Jährlich* bietet umfangreiche statistische Informationen zu ausgewählten Hardware-Komponenten für die letzten zwölf Monate. Die Histogramme werden unter *Täglich* beschrieben.

17.3 Netzwerknutzung

Die Registerkarten des Menüs *Protokolle & Berichte* > *Netzwerknutzung* bieten für verschiedene Zeiträume einen statistischen Überblick über den Datenverkehr, der jede Schnittstelle der Sophos UTM passiert. Zur Darstellung werden die folgenden Maßeinheiten verwendet:

- u (Mikro, 10^{-6})
- m (Milli, 10^{-3})
- k (Kilo, 10^{3})
- M (Mega, 10^{6})
- G (Giga, 10^{9})

Beachten Sie, dass die Skalierung zwischen 10^{-18} und 10^{8} variiert.

17.3.1 Täglich

Die Registerkarte *Netzwerknutzung* > *Täglich* bietet umfangreiche statistische Informationen zum Datendurchsatz jeder konfigurierten Schnittstelle in den letzten 24 Stunden.

Jedes Diagramm enthält zwei grafische Darstellungen:

- **Inbound:** Eingehender Datenverkehr auf dieser Schnittstelle in Bit pro Sekunde.
- **Outbound:** Ausgehender Datenverkehr auf dieser Schnittstelle in Bit pro Sekunde.

Das Diagramm *Gleichzeitige Verbindungen* zeigt die Anzahl der gleichzeitigen Verbindungen.

17.3.2 Wöchentlich

Die Registerkarte *Netzwerknutzung* > *Wöchentlich* bietet umfangreiche statistische Informationen zum Datendurchsatz jeder konfigurierten Schnittstelle in den letzten sieben Tagen. Die Histogramme werden unter *Täglich* beschrieben.

17.3.3 Monatlich

Die Registerkarte *Netzwerknutzung* > *Monatlich* bietet umfangreiche statistische Informationen zum Datendurchsatz jeder konfigurierten Schnittstelle in den letzten vier Wochen. Die Histogramme werden unter *Täglich* beschrieben.

17.3.4 Jährlich

Die Registerkarte *Netzwerknutzung* > *Jährlich* bietet umfangreiche statistische Informationen zum Datendurchsatz jeder konfigurierten Schnittstelle in den letzten zwölf Monaten. Die Histogramme werden unter *Täglich* beschrieben.

17.3.5 Bandbreitennutzung

Die Registerkarte *Netzwerknutzung* > *Bandbreitennutzung* bietet umfangreiche statistische Informationen zu Datenverkehr, der an, von und durch das System gesendet wurde.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Häufigste Clients* oder *Häufigste Dienste nach Client*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *Nach Client* und *Nach Server* können Sie manuell eine IP, ein Netzwerk oder einen Netzwerkbereich (z. B. `192.168.1.0/24` oder `10/8`) eingeben. Bei den Ansichten *nach Dienst* können Sie ein Protokoll und einen Dienst, getrennt durch ein Komma, angeben (z. B. *TCP,SMTP*, *UDP,6000*). Ohne Angabe des Protokolls wird automatisch von TCP ausgegangen (*HTTP* ist z. B. auch gültig).

Wenn Sie in den Ansichten *Häufigste Clients* und *Häufigste Server* auf eine IP oder einen Hostnamen in der Ergebnistabelle klicken, wird diese(r) automatisch als Filter für die Ansicht

Häufigste Dienste nach Client oder *Häufigste Dienste nach Server* verwendet. Wenn Sie in den Ansichten *Häufigste Dienste*, *Häufigste Anwendungen* und *Häufigste Anwendungskategorien* auf einen Dienst, eine Anwendung oder eine Anwendungskategorie in der Ergebnistabelle klicken, wird diese(r) automatisch als Filter für die Ansicht *Häufigste Clients nach Dienst*, *Häufigste Clients nach Anwendung* oder *Häufigste Clients nach Kategorie* verwendet.

Häufigste Anwendungen/Häufigste Anwendungskategorien: Ist Application Control deaktiviert, wird der Netzwerkverkehr als „nicht klassifiziert“ angezeigt. Ist Application Control aktiviert, wird der Netzwerkverkehr nach Typ angezeigt, z. B. „WebAdmin“, „NTP“, „facebook“ usw. Weitere Informationen zu Application Control finden Sie im Kapitel *Web Protection* > *Application Control*.

Bitte beachten Sie, dass die Bezeichnungen *EIN* und *AUS* für Datenverkehr je nach Betrachtungsweise variieren können. Wenn der Proxy eingeschaltet ist, verbinden sich die Clients auf Port `8080` mit der UTM (auch im Transparenzmodus), sodass Daten, die von den Clients gesendet werden (die Anfrage), auf der internen Netzwerkschnittstelle als *eingehender* Verkehr, und Daten, die an den Client gesendet werden (die Antwort), als *ausgehender* Verkehr angesehen werden.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken. Um beispielsweise alle Hosts nach dem eingehenden Verkehr zu sortieren, klicken Sie in der Tabellenüberschrift auf *EIN*. Der Host mit dem meisten Datenverkehr wird dann ganz oben angezeigt. Beachten Sie, dass die Informationen für den Datenverkehr in Kibibyte (KiB) und Mebibyte (MiB), beides Computerspeicher-Einheiten mit der Basis 2, angegeben sind (z. B. 1 Kibibyte = 2^{10} Byte = 1024 Byte).

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.4 Network Protection

Die Registerkarten des Menüs *Protokolle & Berichte* > *Network Protection* bieten einen statistischen Überblick über Ereignisse im Angriffschutzsystem des Netzwerks, die von Sophos

UTM registriert wurden.

17.4.1 Täglich

Die Registerkarte *Network Protection* > *Täglich* bietet umfangreiche statistische Informationen zu den folgenden Ereignissen der letzten 24 Stunden:

- Firewallverstöße
- Intrusion-Prevention-Ereignisse

Firewall-Verletzungen: Jedes verworfene oder abgelehnte Datenpaket wird als Verletzung der Firewall-Regeln gewertet. Die Anzahl der Firewallverstöße wird über einen Zeitraum von fünf Minuten errechnet.

Angriffsschutz-Ereignisse: Alle Diagramme weisen zwei Linien auf:

- **Alert Events (Alarme):** Die Anzahl der Datenpakete, die einen Angriff-Alarm ausgelöst haben.
- **Drop Events (Verwürfe):** Die Anzahl der Datenpakete, die durch das Angriffsschutzsystem verworfen wurden.

17.4.2 Wöchentlich

Auf der Registerkarte *Network Protection* > *Wöchentlich* erhalten Sie einen statistischen Überblick über Firewallverstöße und Ereignisse im Angriffschutzsystem der letzten sieben Tage.Die Histogramme werden unter *Täglich* beschrieben.

17.4.3 Monatlich

Auf der Registerkarte *Network Protection* > *Monatlich* erhalten Sie einen statistischen Überblick über Firewallverstöße und Ereignisse im Angriffschutzsystem der letzten vier Wochen.Die Histogramme werden unter *Täglich* beschrieben.

17.4.4 Jährlich

Auf der Registerkarte *Network Protection* > *Jährlich* erhalten Sie einen statistischen Überblick über Firewallverstöße und Ereignisse im Angriffschutzsystem der letzten zwölf Monate.Die Histogramme werden unter *Täglich* beschrieben.

17.4.5 Firewall

Die Registerkarte *Network Protection > Firewall* stellt umfassende Daten über die Firewall-Aktivitäten, aufgeschlüsselt nach Quell-IP, Quellhosts, Anzahl empfangener Pakete und Anzahl von Diensten, bereit.

Hinweis – Pakete mit einer TTL kleiner oder gleich eins werden verworfen, ohne protokolliert zu werden.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Häufigste Quellhosts* oder *Häufigste Dienste nach Ziel*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *Nach Quelle* und *Nach Ziel* können Sie manuell eine IP, ein Netzwerk oder einen Netzwerkbereich (z. B. `192.168.1.0/24` oder `10/8`) eingeben. In den Ansichten *nach Dienst* können Sie ein Protokoll und einen Dienst, getrennt durch ein Komma, angeben (z. B. *TCP,SMTP* oder *UDP,6000*).

Wenn Sie in den Ansichten *Häufigste Quellhosts* und *Häufigste Zielhosts* auf eine IP oder einen Hostnamen in der Ergebnistabelle klicken, wird diese(r) automatisch als Filter für die Ansicht *Häufigste Dienste nach Quelle* oder *Häufigste Dienste nach Ziel* verwendet. Wenn Sie in der Ansicht *Häufigste Dienste* auf einen Dienst in der Ergebnistabelle klicken, wird dieser automatisch als Filter für die Ansicht *Häufigste Quellhosts nach Diensten* verwendet.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.4.6 Advanced Threat Protection

Auf der Registerkarte *Network Protection > Advanced Threat Protection* finden Sie umfassende Daten zu komplexen Bedrohungen in Ihrem Netzwerk.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Neueste Infektionen* oder *Neueste Infektionen nach Host*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *Neueste von Schadsoftware Infizierte* und *Neueste Infektionen nach Schadsoftware* können Sie manuell nach konkreten Bedrohungen filtern. In den Ansichten *Neueste Infektionen nach Host* können Sie manuell nach einem konkreten Host filtern.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.4.7 IPS

Die Registerkarte *Network Protection > IPS* bietet umfangreiche Daten zu Intrusion-Prevention- (dt. Angriffsschutz-)Aktivitäten in Ihrem Netzwerk.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Häufigste Quellhosts* oder *Häufigste Ziele nach Quelle*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *Nach Quelle* und *Nach Ziel* können Sie manuell eine IP, ein Netzwerk oder einen Netzwerkbereich (z. B. `192.168.1.0/24` oder `10/8`) eingeben. Wenn Sie in den Ansichten *Häufigste Quellhosts* und *Häufigste Zielhosts* auf eine IP in der Ergebnistabelle klicken, wird

diese(r) automatisch als Filter für die Ansicht *Häufigste Ziele nach Quelle* oder *Häufigste Quellen nach Ziel* verwendet.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.5 Web Protection

Das Menü *Protokolle & Berichte* > *Web Protection* bietet einen statistischen Überblick über die aktivsten Internetnutzer und die am häufigsten aufgerufenen Websites.

17.5.1 Internetnutzung

Die Seite *Protokolle & Berichte* > *Web Protection* > *Internetnutzung* bietet Ihnen vielseitige Funktionen, mit denen Sie sich gezielt über Ihren Netzwerkverkehr und die Nutzung des Internets durch Ihre Benutzer informieren können. Auf den ersten Blick wirkt die Seite kompliziert, ihre Verwendung erschließt sich jedoch problemlos durch Ausprobieren.

Web-Surfing-Datenstatistik

Die Erfassung der Web-Surf-Daten erfolgt sitzungsbasiert.UTM unterscheidet zwischen Sitzungen pro Benutzer („Wie lange ist dieser Benutzer im Internet gesurft?“) und Sitzungen pro Benutzer und Domäne („Wie lange ist dieser Benutzer in dieser Domäne gesurft?“), wobei es sich bei der Domäne um die Top-Level-Domäne plus einer weiteren wichtigen Ebene handelt. Um aussagekräftige Näherungswerte zu bekommen, werden alle Daten folgendermaßen erfasst: Jede Web-Anfrage wird anhand des Datenvolumens und der Zeitspanne zwischen Anfragen protokolliert. Wenn für eine Dauer von fünf Minuten keine Anfrage erfasst wurde, gilt die Sitzung als beendet. Damit im Näherungswert berücksichtigt wird, dass der Benutzer die Internetseite eventuell angeschaut hat, auch wenn die Verbindung inaktiv war, wird jeweils eine Minute beim Wert der *Verweildauer* hinzugefügt. Die Berichtsdaten werden alle 15 Minuten aktualisiert.

Das heißt, wenn ein Benutzer z. B. 10 Minuten lang zwischen zwei Domänen wechselt, werden für den Benutzer insgesamt 10 Minuten erfasst; für die Domänen, auf denen der Benutzer gesurft ist, werden jedoch 20 Minuten aufgezeichnet. Wenn der Benutzer verschiedene Tabs oder Browser zum Surfen auf ein- und derselben Domäne verwendet, so hat dies keinen Einfluss auf das Ergebnis.

Wenn Clients versuchen, ungültige URLs anzufragen, werden diese vom Webfilter protokolliert, aber es kann keine Verbindung mit diesen Seiten hergestellt werden. Die Links werden als Fehler gezählt. Dies sind allerdings keine Fehler der Berichtsfunktion oder des Webfilters; in den meisten Fällen treten diese Fehler auf, wenn auf einer Internetseite ungültige oder unvollständige Links enthalten sind.

Seitenaufbau

Kopfzeile

Zunächst gibt es die Kopfzeile mit folgenden Elementen:

- **Home:** Mithilfe dieses Symbols gelangen Sie zurück zum Anfang, frei von sämtlichen Klicks und Filtern.
- **Vorwärts/Rückwärts:** Mithilfe dieser Symbole können Sie im Verlauf Ihrer Änderungen und Einstellungen vor- und zurückblättern. Die Funktion ähnelt der eines Webbrowsers.
- **Verfügbare Berichte:** Diese Auswahlliste enthält alle verfügbaren Berichtstypen, einschließlich (falls vorhanden) Ihrer eigenen gespeicherten Berichte.Sie ist standardmäßig auf *Sites* eingestellt. Der Inhalt der Ergebnistabelle auf der Seite *Internetnutzung* hängt unmittelbar von dieser Berichtstyp-Einstellung ab.

  > **Hinweis –** Wenn Sie Filter verwenden und anschließend die Berichte durchgehen, sehen Sie, dass die Einstellung *Verfügbare Berichte* automatisch geändert wurde. Sie zeigt stets die jeweils aktuelle Berichtsgrundlage an.

  Standard: Es stehen mehrere Berichtstypen zur Verfügung; ausführlichere Informationen hierzu finden Sie weiter unten.

  Gespeicherte Webberichte: Hier können Sie gespeicherte Webberichte auswählen, die Sie bereits erstellt haben.
- **Löschen:** Klicken Sie auf dieses Symbol, um einen gespeicherten Webbericht zu löschen. Standardberichte können nicht gelöscht werden.

- **Speichern:** Klicken Sie auf dieses Symbol, um eine aktuelle Ansicht zu speichern und sie später erneut aufrufen zu können.Sie wird in der Auswahlliste *Verfügbare Berichte* gespeichert.

Filterleiste

In der Filterleiste befinden sich folgende Elemente:

- **Plus:** Klicken Sie auf dieses Symbol, um zusätzliche Filter zu erstellen; ausführlichere Informationen hierzu finden Sie weiter unten.
- **Anzahl:** Verwenden Sie die Auswahlliste, um die Anzahl der Ergebnisse in der Tabelle zu reduzieren. Sie können jeweils die ersten 10, die ersten 50 oder die ersten 100 Ergebnisse anzeigen.
- **Zeit:** Verwenden Sie die Auswahlliste, um die Ergebnisse in der Tabelle auf bestimmte Zeiträume einzugrenzen oder zu erweitern. Der Berichtszeitraum *Angepasst* ermöglicht es Ihnen, eigene Zeiträume festzulegen.
- **Abteilungen:** Verwenden Sie die Auswahlliste, um die Ergebnisse in der Tabelle auf bestimmte Abteilungen einzugrenzen. Auf der Seite *Abteilungen* können Sie Abteilungen erstellen.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol auf der rechten Seite der Filterleiste klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol oberhalb der Tabelle klicken. Wenn Sie auf das Senden-Symbol klicken, wird ein Dialogfenster geöffnet, in das Sie einen oder mehrere Empfänger eingeben können, an die dieser Bericht per E-Mail gesendet werden soll. Sie können einen Betreff und einen Nachrichtentext eingeben. Sie können selbst auch regelmäßig gespeicherte Berichte empfangen; weitere Informationen hierzu finden Sie im Abschnitt *Geplante Berichte*.

Ergebnistabelle

Ganz unten befindet sich die Ergebnistabelle.Was darin angezeigt wird, hängt erstens vom ausgewählten Berichtstyp (die jeweils aktuelle Einstellung wird in der Liste *Verfügbare Berichte* angezeigt) und zweitens von gegebenenfalls definierten Filtern ab.

> **Hinweis –** Bei aktivierter Anonymisierung werden die Benutzer nicht mit Namen oder IP-Adresse, sondern nummeriert angezeigt.

Je nach ausgewähltem Berichtstyp enthält die Tabelle verschiedene Informationen:

	Benutzer	**Kategorien**	**Sites**	**Domänen**	**URLs**	**Blockierungs-Umgehungen (engl. over-rides)**
#	✓	✓	✓	✓	✓	✓
Verkehr	✓	✓	✓	✓	✓	
%	✓	✓	✓	✓	✓	
Dauer	✓		✓			
Seiten	✓	✓	✓			
Anfragen	✓	✓	✓	✓	✓	
Benutzer						✓
Site						✓
Kategorien*					✓	✓
Aktion*					✓	✓
Ursache*					✓	✓
Info*					✓	✓

* = Diese Zellen können angeklickt werden, um weitere, detailliertere Informationen anzuzeigen.

#: Platzierung im Hinblick auf das Datenverkehrsaufkommen.

Verkehr: Umfang des Datenverkehrsaufkommens.

%: Anteil am Gesamtdatenverkehr in Prozent.

Dauer: Benutzerberichtstyp: Verweildauer nach Benutzer(n). Site-Berichtstyp: Gesamtverweildauer (Summe aller Benutzer) auf der/den Website(s).

Seiten: Zahl der angefragten Seiten (d. h. alle Anfragen, die mit Code 200 und Inhaltstyp-Text/html beantwortet wurden).

Anfragen: Anzahl der Web-Anfragen pro Kategorie, Site, Domäne oder URL.

Benutzer: Name des Benutzers, der die Blockierung umgangen hat.Falls Anonymisierung aktiv ist, wird *user_#* angezeigt.

Site: Website, für die Blockierung umgangen wurde.

Kategorien: Zeigt alle Kategorien an, denen eine URL angehört. Bei mehreren Kategorien wird durch Anklicken der Kategorie ein kleines Dialogfeld geöffnet. Aus diesem können Sie anschließend eine Kategorie auswählen, auf deren Basis dann ein Filter erstellt wird.

Aktion: Zeigt an, ob die Website an den Client übermittelt wurde (*zugelassen* – passed), ob sie durch eine Application-Control-Regel *blockiert* wurde oder ob sie von einem Benutzer mit Hilfe der Blockierungs-Umgehung (Bypass Blocking) geöffnet wurde (*overridden*).

Ursache: Zeigt an, warum eine Website-Anfrage blockiert wurde oder warum die Blockierung umgangen wurde.Beispiel: Ein Benutzer versucht, eine `msi`-Datei herunterzuladen. Es existiert jedoch eine Application-Control-Regel, die Dateiübertragungen verhindert. In diesem Fall wird in der Zelle *msi* als Ursache angezeigt. Bei umgangenen Blockierungen wird der Grund angezeigt, der vom Benutzer angegeben wurde.

Info: Diese Zelle enthält (falls verfügbar) zusätzliche Informationen darüber, warum eine Website-Anfrage blockiert wurde. Wurde z. B. der Download einer Datei aufgrund ihrer Erweiterung blockiert, enthält die Zelle das Wort *Erweiterung*.

Definition von Filtern

Filter werden verwendet, um in der Ergebnistabelle Informationen mit bestimmten Eigenschaften anzuzeigen. Für die Definition von Filtern stehen zwei Möglichkeiten zur Verfügung: Anklicken des Plussymbols in der Filterleiste oder Klicken in die Tabelle.

Definition über das Plus-Symbol: Nach Anklicken des grünen Plus-Symbols in der Filterleiste wird ein kleines Filterdialogfeld mit zwei Feldern angezeigt.Im ersten Feld, einer Auswahlliste, können Sie einen Berichtstyp auswählen, zum Beispiel *Kategorie*. Im zweiten Feld können Sie dann einen Wert für den ausgewählten Berichtstyp wählen oder eingeben, z. B. *Erwachseneninhalte*, wenn *Kategorie* ausgewählt ist. Klicken Sie auf *Speichern*, um den Filter zu speichern und gleichzeitig auf die Ergebnistabelle anzuwenden.

Definition über die Tabelle: Durch Klicken in die Tabelle öffnet sich das Dialogfenster *Berichtaufschlüsselung*, wenn für den von Ihnen angeklickten Eintrag mehr als ein Berichtstyp zur Verfügung steht. Sie müssen eine der angezeigten Filteroptionen auswählen. Anschließend wird das Fenster *Berichtaufschlüsselung* geschlossen, der jeweilige Filter erstellt und in der Filterleiste angezeigt. In der Ergebnistabelle werden jetzt die neuen, gefilterten Ergebnisse angezeigt.
Beispiel: Auf der Seite *Internetnutzung* wird standardmäßig der Bericht *Sites* angezeigt. Klicken Sie in der Ergebnistabelle in eine beliebige Zeile (z. B. amazon.com). Das Dialogfenster *Berichtaufschlüsselung* wird geöffnet. Sie können drei verschiedene Optionen auswählen: Sie können für die jeweilige Site entweder Informationen über *Domänen*, *Benutzer*, welche die Site

besucht haben, oder *Kategorien*, denen die Site angehört, anzeigen. Sie sehen, dass zahlreiche Benutzer amazon.com besucht haben und möchten mehr über diese Website erfahren, also aktivieren Sie das Feld *Benutzer*. Das Fenster wird geschlossen. Sie sehen in der Kopfleiste, dass der Berichtstyp in *Benutzer* geändert wurde, und in der Filterleiste, dass die Informationen in der Ergebnistabelle für *Benutzer* nach der von Ihnen ausgewählten Website (amazon.com) gefiltert sind. Die Tabelle zeigt nun alle Benutzer an, die diese Website besucht haben, sowie zusätzliche Informationen über ihre Sitzungen.

Hinweis – Manchmal kommt es darauf an, in welche Tabellenzeile Sie klicken, da bestimmte Zellen über eigene Filter verfügen (weitere Informationen hierzu finden Sie bei den Einträgen mit Asterisk (*) oben im Abschnitt *Ergebnistabelle*).

17.5.2 Suchmaschinen

Die Seite *Protokolle & Berichte* > *Web Protection* > *Suchmaschinen* enthält Informationen über die Suchmaschinen, die Ihre Benutzer verwenden, und die Recherchen, die sie damit durchführen. Auf den ersten Blick wirkt die Seite kompliziert, ihre Verwendung erschließt sich jedoch problemlos durch Ausprobieren.

Seitenaufbau

Kopfzeile

Zunächst gibt es die Kopfzeile mit folgenden Elementen:

- **Home:** Mithilfe dieses Symbols gelangen Sie zurück zum Anfang, frei von sämtlichen Klicks und Filtern.
- **Vorwärts/Rückwärts:** Mithilfe dieser Symbole können Sie im Verlauf Ihrer Änderungen und Einstellungen vor- und zurückblättern. Die Funktion ähnelt der eines Webbrowsers.
- **Verfügbare Berichte:** Diese Auswahlliste enthält alle verfügbaren Berichtstypen, einschließlich (falls vorhanden) Ihrer eigenen gespeicherten Berichte.Sie ist standardmäßig auf *Recherchen* eingestellt.Der Inhalt der Ergebnistabelle auf der Seite *Suchmaschinen* hängt unmittelbar von dieser Berichtstyp-Einstellung ab.

> **Hinweis –** Wenn Sie Filter verwenden und anschließend die Berichte durchgehen, sehen Sie, dass die Einstellung *Verfügbare Berichte* automatisch geändert wurde. Sie zeigt stets die jeweils aktuelle Berichtsgrundlage an.

Standard: Es stehen drei Berichtstypen zur Verfügung; ausführlichere Informationen hierzu finden Sie weiter unten.

Gespeicherte Suchmaschinenberichte: Hier können Sie gespeicherte Suchmaschinenberichte auswählen, die Sie bereits erstellt haben.

- **Löschen:** Klicken Sie auf dieses Symbol, um einen gespeicherten Suchmaschinenbericht zu löschen. Standardberichte können nicht gelöscht werden.
- **Speichern:** Klicken Sie auf dieses Symbol, um eine aktuelle Ansicht zu speichern und sie später erneut aufrufen zu können.Sie wird in der Auswahlliste *Verfügbare Berichte* gespeichert.

Filterleiste

In der Filterleiste befinden sich folgende Elemente:

- **Plus:** Klicken Sie auf dieses Symbol, um zusätzliche Filter zu erstellen; ausführlichere Informationen hierzu finden Sie weiter unten.
- **Anzahl:** Verwenden Sie die Auswahlliste, um die Anzahl der Ergebnisse in der Tabelle zu reduzieren. Sie können jeweils die ersten 10, die ersten 50 oder die ersten 100 Ergebnisse anzeigen.
- **Zeit:** Verwenden Sie die Auswahlliste, um die Ergebnisse in der Tabelle auf bestimmte Zeiträume einzugrenzen oder zu erweitern. Der Berichtszeitraum *Angepasst* ermöglicht es Ihnen, eigene Zeiträume festzulegen.
- **Abteilungen:** Verwenden Sie die Auswahlliste, um die Ergebnisse in der Tabelle auf bestimmte Abteilungen einzugrenzen. Auf der Seite *Abteilungen* können Sie Abteilungen erstellen.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol auf der rechten Seite der Filterleiste klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol oberhalb der Tabelle klicken. Wenn Sie auf das Senden-Symbol klicken, wird ein Dialogfenster geöffnet, in das Sie einen oder mehrere Empfänger eingeben können, an die dieser Bericht per E-Mail gesendet werden soll. Sie können einen Betreff und einen Nachrichtentext eingeben. Sie können selbst auch regelmäßig

gespeicherte Berichte empfangen; weitere Informationen hierzu finden Sie im Abschnitt *Geplante Berichte*.

Ergebnistabelle

Ganz unten befindet sich die Ergebnistabelle.Was darin angezeigt wird, hängt erstens vom ausgewählten Berichtstyp (die jeweils aktuelle Einstellung wird in der Liste *Verfügbare Berichte* angezeigt) und zweitens von gegebenenfalls definierten Filtern ab. Die folgenden Berichtstypen sind verfügbar:

- **Recherchen:** Zeigt die Suchbegriffe an, die Ihre Benutzer verwendet haben.
- **Suchmaschinen:** Zeigt die Suchmaschinen an, die Ihre Benutzer verwendet haben.
- **Benutzerrecherchen:** Zeigt die Benutzer an, die Recherchen durchgeführt haben.

Hinweis – Bei aktivierter Anonymisierung werden die Benutzer nicht mit Namen oder IP-Adresse, sondern nummeriert angezeigt.

Die Tabelle enthält die folgenden Informationen über jeden Berichtstyp:

#: Platzierung im Hinblick auf die Häufigkeit.

Anfragen: Anzahl der Anfragen pro Suchbegriff, Suchmaschine oder Benutzer.

%: Anteil an der Gesamtzahl der Recherchen in Prozent.

Definition von Filtern

Filter werden verwendet, um in der Ergebnistabelle Informationen mit bestimmten Eigenschaften anzuzeigen. Für die Definition von Filtern stehen zwei Möglichkeiten zur Verfügung: Anklicken des Plussymbols in der Filterleiste oder Klicken in die Tabelle.

Definition über das Plus-Symbol: Nach Anklicken des grünen Plus-Symbols in der Filterleiste wird ein kleines Filterdialogfeld mit zwei Feldern angezeigt.Im ersten Feld, einer Auswahlliste, können Sie einen Berichtstyp auswählen, zum Beispiel *Suchmaschine*.Im zweiten Feld können Sie einen Wert für den ausgewählten Berichtstyp wählen oder eingeben, z. B. *Google (google.com)*, wenn *Suchmaschine* ausgewählt ist.Klicken Sie auf *Speichern*, um den Filter zu speichern und gleichzeitig auf die Ergebnistabelle anzuwenden. Beachten Sie bei der Eingabe von Suchbegriffen die Groß- und Kleinschreibung; Platzhalter werden unterstützt: '*' für die Suche nach null oder mehr Zeichen und '?' für die Suche nach einem Zeichen.

Definition über die Tabelle: Durch Klicken in die Tabelle öffnet sich das Dialogfenster *Berichtaufschlüsselung*, wenn für den von Ihnen angeklickten Eintrag mehr als ein Berichtstyp zur Verfügung steht. Sie müssen eine der angezeigten Filteroptionen auswählen. Anschließend wird das Fenster *Berichtaufschlüsselung* geschlossen, der jeweilige Filter erstellt und in der Filterleiste angezeigt. In der Ergebnistabelle werden jetzt die neuen, gefilterten Ergebnisse angezeigt.
Beispiel: Auf der Seite *Suchmaschinen* wird standardmäßig der Bericht *Recherchen* angezeigt. Klicken Sie in der Ergebnistabelle in eine beliebige Zeile (z. B. Wetter).Das Dialogfenster *Berichtaufschlüsselung* wird geöffnet. Sie können zwischen zwei Optionen wählen. Sie können Informationen über die für die Recherche verwendeten Suchmaschinen (*Suchmaschinen*) oder über die Benutzer, welche diesen Suchbegriff verwendet haben (*Recherche-Benutzer*), anzeigen.Sie sehen, dass zahlreiche Benutzer den Suchbegriff „Wetter“ verwendet haben und möchten mehr darüber erfahren, also aktivieren Sie das Feld *Recherche-Benutzer*. Das Fenster wird geschlossen.Sie sehen in der Kopfleiste, dass der Berichtstyp in *Recherche-Benutzer* geändert wurde, und in der Filterleiste, dass die Informationen in der Ergebnistabelle für *Recherche-Benutzer* nach dem von Ihnen ausgewählten Suchbegriff (Wetter) gefiltert sind. Die Tabelle zeigt nun alle Benutzer an, die den Suchbegriff „Wetter“ verwendet haben sowie zusätzliche Informationen über ihre Recherchen.

17.5.3 Abteilungen

Auf der Seite *Protokolle & Berichte* > *Web Protection* > *Abteilungen* können Sie Benutzer oder Hosts und Netzwerke in virtuelle Abteilungen gruppieren. Diese Abteilungen können dann zum Filtern von Internetnutzungs- oder Suchmaschinenberichten verwendet werden.

Um eine Abteilung anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Abteilungen* auf *Abteilung hinzufügen*.**
   Das Dialogfeld *Neue Abteilung hinzufügen* wird geöffnet.

2. **Geben Sie einen Namen ein**.

   Geben Sie in das Feld *Name* einen aussagekräftigen Namen für die Abteilung ein.

3. **Fügen Sie Benutzer oder Hosts/Netzwerke hinzu.**
   Eine Abteilungsdefinition kann immer nur entweder Benutzer oder Hosts/Netzwerke enthalten, nicht beide gleichzeitig.

   - **Benutzer:** Fügen Sie einen oder mehrere Benutzer, die dieser Abteilung angehören sollen, zum Feld hinzu.

- **Hosts/Netzwerke:** Fügen Sie einen oder mehrere Hosts oder Netzwerke, die dieser Abteilung angehören sollen, zum Feld hinzu.

  Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

4. **Klicken Sie auf *Speichern*.**
   Die neue Abteilung wird in der Liste *Abteilungen* angezeigt.

Um eine Abteilung zu bearbeiten, zu löschen oder zu klonen, klicken Sie auf die entsprechenden Schaltflächen.

Weitere Informationen zur Verwendung von Abteilungen finden Sie in den Abschnitten *Internetnutzung* und *Suchmaschinen*.

17.5.4 Geplante Berichte

Auf der Seite *Protokolle & Berichte > Web Protection > Geplante Berichte* können Sie festlegen, welche Ihrer gespeicherten Berichte regelmäßig per E-Mail versendet werden sollen. Bevor Sie einen geplanten Bericht erstellen können, müssen Sie über mindestens einen gespeicherten Bericht verfügen (weitere Informationen zum Speichern von Berichten finden Sie in den Abschnitten *Internetnutzung* oder *Suchmaschinen*).

Um einen geplanten Bericht anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Geplante Berichte* auf *Geplanten Bericht hinzufügen*.**
   Das Dialogfeld *Neuen geplanten Bericht hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den geplanten Bericht ein.

   Intervall: Wählen Sie aus der Auswahlliste ein Zeitintervall zum Versenden des oder der Berichte.

   Berichte: Alle gespeicherten Berichte sind hier aufgeführt. Markieren Sie das Auswahlkästchen vor jedem Bericht, der im ausgewählten Zeitintervall versendet werden soll.

   Empfänger: Fügen Sie alle Empfänger, die den/die ausgewählte(n) Bericht(e) erhalten sollen, in das Feld ein. Beachten Sie, dass Sie mit Hilfe der Importschaltfläche auch eine ganze Liste an Empfängern hinzufügen können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen hinzu.

3. **Klicken Sie auf *Speichern*.**

   Der neue geplante Bericht wird in der Liste *Geplante Berichte* angezeigt.

Um einen geplanten Bericht zu bearbeiten, zu löschen oder zu klonen, klicken Sie auf die entsprechenden Schaltflächen. Verwenden Sie den Schieberegler eines Berichts, um den Versand von Berichten zu deaktivieren, ohne den Bericht selbst zu löschen.

17.5.5 Application Control

Die Seite *Protokolle & Berichte* > *Web Protection* > *Application Control* bietet umfangreiche statistische Informationen zu den aktivsten Quellen, den am häufigsten aufgerufenen Zielen und den beliebtesten Anwendungen für verschiedene Zeiträume.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Häufigste Quellen* oder *Häufigste Anwendungen*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *Nach Quelle* und *Nach Ziel* können Sie manuell eine IP, ein Netzwerk oder einen Netzwerkbereich (z. B. `192.168.1.0/24` oder `10/8`) eingeben. In den Ansichten *nach Dienst* können Sie ein Protokoll und einen Dienst, getrennt durch ein Komma, angeben (z. B. *TCP,SMTP* oder *UDP,6000*).

Wenn Sie in der Ansicht *Häufigste Quellen* auf eine IP oder einen Hostnamen in der Ergebnistabelle klicken, wird diese(r) automatisch als Filter für die Ansicht *Häufigste Anwendungen nach Quelle* verwendet. Wenn Sie in den Ansichten *Häufigste Anwendungen* und *Häufigste Anwendungskategorien* auf eine Anwendung oder Anwendungskategorie in der Ergebnistabelle klicken, wird diese automatisch als Filter für die Ansicht *Häufigste Quellen nach Anwendung* oder *Häufigste Quellen nach Anwendungskategorie* verwendet.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

Die aktivsten Quellen werden nicht sofort in der Übersicht angezeigt, sondern erst nachdem eine Sitzungs-Zeitüberschreitung stattgefunden hat. Dies ist der Fall, wenn ein bestimmter Client (Benutzername oder IP-Adresse) für fünf Minuten das Surfen im Internet unterbricht. UTM erklärt diese Verbindung für „tot" und sendet die Information an eine Datenbank, bevor sie in die Liste der aktivsten Quellen aufgenommen wird.

17.5.6 Entanonymisierung

Auf die Registerkarte *Web Protection > Entanonymisierung* kann nur zugegriffen werden, wenn Anonymisierung aktiviert ist (siehe *Protokolle & Berichte > Berichtseinstellungen > Anonymisierung*).

Hier ist es möglich, die Anonymisierung für bestimmte Benutzer im Hinblick auf Web-Protection-Berichte auszusetzen. Gehen Sie folgendermaßen vor:

1. **Geben Sie beide Kennwörter ein.**
   Geben Sie das erste und das zweite Kennwort ein, die zur Aktivierung der Anonymisierung angegeben wurden.
2. **Fügen Sie Benutzer hinzu, die entanonymisiert werden sollen.**
   Fügen Sie zum Feld *Benutzer entanonymisieren* die Benutzernamen von jenen Benutzern hinzu, die Sie entanonymisieren wollen.
3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

17.6 Email Protection

Die Registerkarten des Menüs *Protokolle & Berichte > Email Protection* bieten einen statistischen Überblick über den E-Mail-Verkehr, die E-Mail-Nutzung und die E-Mail-Sicherheit.

17.6.1 Nutzungsdiagramme

Die Registerkarte *Email Protection > Nutzungsdiagramme* bietet einen statistischen Überblick über den E-Mail-Verkehr auf der UTM für verschiedene Zeiträume:

- Täglich
- Wöchentlich
- Monatlich
- Jährlich

17.6.2 Mail-Nutzung

Die Registerkarte *Email Protection > Mail-Nutzung* bietet umfangreiche statistische Informationen zu den am häufigsten genutzten E-Mail-Adressen und Adressdomänen für verschiedene Zeiträume.

Wählen Sie in der ersten Auswahlliste die Art der Daten aus, die Sie anzeigen möchten, z. B. *Häufigste Absender* oder *Häufigste Domänen*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *nach Domäne* und *nach Adresse* können Sie manuell eine Domäne bzw. eine Adresse angeben. Beachten Sie, dass Sie beim Angeben von Domänen das Prozentzeichen (`%`) als Platzhalter verwenden können. Wenn Sie ein Prozentzeichen nach Ihrem Suchbegriff einfügen, sucht Sophos UTM nach genauen Treffern und teilweisen Übereinstimmungen. Beachten Sie, dass das Filterfeld zwischen Groß- und Kleinschreibung unterscheidet.

Wenn Sie in den Ansichten *Häufigste Adressen* und *Häufigste Domänen* auf eine Adresse oder eine Domäne in der Ergebnistabelle klicken, wird diese automatisch als Filter für die Ansicht *Häufigste Adressen nach Domäne* oder *Häufigste Peers nach Adresse* verwendet.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.6.3 Blockierte Mails

Die Registerkarte *Email Protection > Blockierte Mails* bietet umfangreiche statistische Informationen zu allen blockierten E-Mail-Anfragen, die auf Antivirus und Antispam basieren.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Häufigster Grund blockierter Spams* oder *Häufigste blockierte Schadsoftware*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

Wenn Sie in der Ansicht *Häufigste blockierte Domäne* auf eine Domäne in der Ergebnistabelle klicken, wird diese automatisch als Filter für die Ansicht *Häufigste blockierte Adressen nach Domäne* verwendet. In der Ansicht *nach Domäne* können Sie manuell eine Domäne angeben. Beachten Sie, dass Sie das Prozentzeichen (`%`) als Platzhalter verwenden können. Wenn Sie ein Prozentzeichen nach Ihrem Suchbegriff einfügen, sucht Sophos UTM nach genauen Treffern und teilweisen Übereinstimmungen. Beachten Sie, dass das Filterfeld zwischen Groß- und Kleinschreibung unterscheidet.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.6.4 Entanonymisierung

Auf die Registerkarte *Email Protection > Entanonymisierung* kann nur zugegriffen werden, wenn Anonymisierung aktiviert ist (siehe *Protokolle & Berichte > Berichtseinstellungen > Anonymisierung*).

Hier ist es möglich, die Anonymisierung für bestimmte E-Mail-Adressen und/oder -Domänen im Hinblick auf Email-Protection-Berichte auszusetzen. Gehen Sie folgendermaßen vor:

1. **Geben Sie beide Kennwörter ein.**
   Geben Sie das erste und das zweite Kennwort ein, die zur Aktivierung der Anonymisierung angegeben wurden.

2. **Nehmen Sie die folgenden Einstellungen vor:**
   Adressen entanonymisieren: Sie können E-Mail-Adressen hinzufügen, die Sie entanonymisieren wollen.

   Domänen entanonymisieren: Sie können Domänen hinzufügen, die Sie entanonymisieren wollen.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

   Die angegebenen E-Mail-Adressen und Domänen sind in Berichten nun lesbar.

17.7 Wireless Protection

Die Registerkarten des Menüs *Protokolle & Berichte* > *Wireless Protection* bieten einen statistischen Überblick über Wireless-Protection-Ereignisse des Netzwerks, die von Sophos UTM registriert wurden.

17.7.1 Täglich

Die Registerkarte *Wireless Protection* > *Täglich* bietet einen statistischen Überblick über die WLAN-Netzwerke und Access Points in den letzten 24 Stunden.

SSID-basierter Bericht

Für jedes WLAN-Netzwerk gibt es ein Diagramm. Jedes Diagramm zeigt zwei Kurven:

- **Verbundene Clients:** Die Anzahl der Clients, die mit dem WLAN-Netzwerk verbunden sind.
- **Fehlgeschlagene Verbindungsversuche:** Die Anzahl der fehlgeschlagenen Verbindungsversuche an dem WLAN-Netzwerk.

AP-basierter Bericht

Für jeden Access Point zeigt die Tabelle die maximale und durchschnittliche Anzahl an verbundenen Benutzern, die Verfügbarkeit (die aufsummierte Zeitdauer, in der der AP während der letzten 24 Stunden verfügbar war) und die Anzahl der Wiedereinwahlen.

17.7.2 Wöchentlich

Die Registerkarte *Wireless Protection* > *Wöchentlich* bietet einen statistischen Überblick über die WLAN-Netzwerke und Access Points in den letzten sieben Tagen. Die Histogramme werden unter *Täglich* beschrieben.

17.7.3 Monatlich

Die Registerkarte *Wireless Protection* > *Monatlich* bietet einen statistischen Überblick über die WLAN-Netzwerke und Access Points in den letzten vier Wochen. Die Histogramme werden unter *Täglich* beschrieben.

17.7.4 Jährlich

Die Registerkarte *Wireless Protection* > *Jährlich* bietet einen statistischen Überblick über die WLAN-Netzwerke und Access Points in den letzten zwölf Monaten. Die Histogramme werden unter *Täglich* beschrieben.

17.8 Fernzugriff

Die Registerkarten des Menüs *Protokolle & Berichte* > *Fernzugriff* bieten einen statistischen Überblick über Fernzugriff-Aktivitäten und Informationen zu Sitzungen.

17.8.1 Aktivität

Die Registerkarte *Fernzugriff* > *Aktivität* bietet umfangreiche statistische Informationen zu den Fernzugriff-Aktivitäten auf der UTM für IPsec, SSL-VPN, PPTP und L2TP über verschiedene Zeiträume:

- Täglich
- Wöchentlich
- Monatlich
- Jährlich

Zeitraum auswählen: Verwenden Sie die Auswahlliste, um einen Berichtszeitraum auszuwählen. Die Seite wird automatisch aktualisiert.

17.8.2 Sitzung

Die Registerkarte *Fernzugriff* > *Sitzung* bietet umfangreiche statistische Informationen zu abgeschlossenen Sitzungen, fehlgeschlagenen Anmeldungen und momentanen Benutzern für verschiedene Zeiträume.

Hinweis – Die Spalten *Hoch* und *Herunter* zeigen Nutzungsdaten der Fernzugriffsverbindungen. Die Erfassung der Nutzungsdaten ist standardmäßig deaktiviert, da dies die Systemlast erhöhen kann. Sie können die Erfassung der Nutzungsdaten auf der Registerkarte *Berichteinstellungen* > *Einstellungen* im Bereich *Fernzugriffs-Nutzungsstatistik* aktivieren.

Wählen Sie in der ersten Auswahlliste die Art der Sitzung, die Sie anzeigen möchten: *Momentane Benutzer*, *Abgeschlossene Sitzungen* oder *Fehlgeschlagene Anmeldeversuche*. Klicken Sie auf *Aktualisieren*, um den Filter anzuwenden.

Mit der zweiten Auswahlliste können Sie die Ergebnisse weiter filtern. Abhängig von der gewählten Art von Sitzungen stehen verschiedene Filter zur Verfügung, z. B. *Nach Dienst* oder *Nach Quell-IP-Adresse*. Für einige Filter müssen Sie ein Filterkriterium eingeben oder auswählen.

Mit der dritten Auswahlliste können Sie die Ergebnisse nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.9 Webserver Protection

Die Registerkarten des Menüs *Protokolle & Berichte* > *Webserver Protection* bieten einen statistischen Überblick über Webserver-Anfragen, Warnhinweise und Alarme.

17.9.1 Nutzungsdiagramme

Die Registerkarte *Webserver Protection* > *Nutzungsdiagramme* bietet einen statistischen Überblick über Webserver-Anfragen, Warnhinweise und Alarme auf UTM für verschiedene Zeiträume:

- Täglich
- Wöchentlich
- Monatlich
- Jährlich

17.9.2 Details

Die Registerkarte *Webserver Protection* > *Details* bietet umfangreiche statistische Informationen zu den aktivsten Clients, virtuellen Hosts, Backends, Antwort-Codes und verschiedenen Angriffen über verschiedene Zeiträume.

Wählen Sie in der ersten Auswahlliste die Art der Daten, die Sie anzeigen möchten, z. B. *Häufigste Clients* oder *Häufigste Angreifer nach virtuellem Host*. Wählen Sie den gewünschten Eintrag und, falls ein zusätzliches Feld angezeigt wird, geben Sie das entsprechende Filterkriterium ein. Sie können die Daten zusätzlich mit Hilfe der Auswahlliste darunter nach Zeit filtern. Klicken Sie immer auf *Aktualisieren*, um die Filter anzuwenden.

In den Ansichten *Nach Client* und *Nach Angreifer* können Sie manuell eine IP, ein Netzwerk oder einen Netzwerkbereich (z. B. `192.168.1.0/24` oder `10/8`) angeben. In der Ansicht *Nach virtuellem Host* können Sie manuell eine Domäne angeben. Beachten Sie, dass Sie das Prozentzeichen (`%`) als Platzhalter verwenden können. Wenn Sie ein Prozentzeichen nach Ihrem Suchbegriff einfügen, sucht Sophos UTM nach genauen Treffern und teilweisen Übereinstimmungen. Beachten Sie, dass das Filterfeld zwischen Groß- und Kleinschreibung unterscheidet.

Wenn Sie in den Ansichten *Häufigste Clients* oder *Häufigste Angreifer* auf eine IP in der Ergebnistabelle klicken, wird diese automatisch als Filter für die Ansicht *Häufigste Antwort-Codes nach Client* oder *Häufigste Regeln nach Angreifer* verwendet.

Standardmäßig werden 20 Einträge pro Seite angezeigt. Wenn es mehr Daten gibt, können Sie mit Hilfe der Vorwärts- und Rückwärts-Symbole durch die Daten navigieren. Mit Hilfe der Auswahlliste *Zeilen pro Seite* können Sie die Anzahl der Einträge pro Seite erhöhen.

Sie können die Daten sortieren, indem Sie auf eine Spaltenüberschrift der Tabelle klicken.

Sie können die Daten im PDF- oder Excel-Format herunterladen, indem Sie auf das entsprechende Symbol in der rechten oberen Ecke der Registerkarte klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert. Zusätzlich können Sie ein Tortendiagramm anzeigen lassen, indem Sie auf das Tortendiagramm-Symbol – falls vorhanden – klicken.

17.10 Gesamtbericht

Im Menü *Protokolle & Berichte > Gesamtbericht* können Sie eine Zusammenstellung der wichtigsten Berichtsdaten erstellen, die in grafischer Form die Netzwerknutzung für eine Reihe von Diensten anzeigt.

17.10.1 Bericht anzeigen

Auf der Registerkarte *Protokolle & Berichte > Gesamtbericht > Bericht anzeigen* können Sie einen kompletten Gesamtbericht erstellen, der aus den einzelnen Berichten auf den Registerkarten und Seiten des Menüs *Berichte* zusammengestellt wird. Klicken Sie auf die Schaltfläche *Bericht jetzt erstellen*, um den Gesamtbericht in einem neuen Fenster zu öffnen.

17.10.2 Archivierte Gesamtberichte

Die Registerkarte *Gesamtbericht > Archivierte Gesamtberichte* bietet einen Überblick über alle archivierten Gesamtberichte. Es werden nur Gesamtberichte archiviert, für die auf der Registerkarte *Konfiguration* die Archivierung aktiv ist.

17.10.3 Konfiguration

Auf der Registerkarte *Gesamtbericht > Konfiguration* können Sie die Einstellungen für die Gesamtberichte vornehmen.

Täglicher Gesamtbericht

Täglicher Gesamtbericht: Ist die Option aktiv, wird ein täglicher Gesamtbericht erstellt.

PDF-Berichte archivieren: Ist die Option ausgewählt, wird der tägliche Gesamtbericht als PDF-Datei archiviert. Archivierte Gesamtberichte stehen auf der Registerkarte *Archivierte Gesamtberichte* zur Verfügung.

Bericht als PDF statt als HTML senden: Ist die Option ausgewählt, wird der Gesamtbericht als PDF-Datei an die E-Mail angehängt. Ist sie nicht ausgewählt, wird er als HTML-Datei versendet.

E-Mail-Adressen: Geben Sie die E-Mail-Adressen der Empfänger ein, die den Gesamtbericht erhalten sollen.

Wöchentlicher Gesamtbericht

Die meisten der Einstellungen sind im Abschnitt *Täglicher Gesamtbericht* beschrieben.

Sie können zusätzlich den Wochentag auswählen, an dem jeweils die Datensammlung für den Gesamtbericht starten soll.

Monatlicher Gesamtbericht

Die Einstellungen sind im Abschnitt *Täglicher Gesamtbericht* beschrieben.

17.11 Protokolleinstellungen

Im Menü *Protokolle & Berichte > Protokolleinstellungen* können Sie die Grundeinstellungen für die lokale und die entfernte Protokollierung festlegen.

17.11.1 Lokale Protokollierung

Auf der Registerkarte *Protokolle & Berichte > Protokolleinstellungen > Lokale Protokollierung* werden die Einstellungen für die lokale Protokollierung vorgenommen. Die lokale Protokollierung ist standardmäßig eingeschaltet.

Falls sie deaktiviert wurde, können Sie sie folgendermaßen wieder einschalten:

1. **Aktivieren Sie die lokale Protokollierung auf der Registerkarte *Lokale Protokollierung*.**
   Klicken Sie auf den Schieberegler.

Der Schieberegler wird grün und die Berichte auf dieser Registerkarte können bearbeitet werden.

2. **Wählen Sie einen Zeitraum, nach dem die Protokolldateien automatisch gelöscht werden sollen.**
   Wählen Sie aus der Auswahlliste eine Aktion, die automatisch auf die Protokolldateien angewendet werden soll. *Protokolldateien nie löschen* ist voreingestellt.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Schwellenwerte

Hier können Sie Schwellenwerte für die lokale Protokollierung festlegen. Diese Schwellenwerte sind an bestimmte Aktionen gekoppelt, welche ausgeführt werden, wenn ein Schwellenwert erreicht ist. Die folgenden Aktionen sind möglich:

- **Nichts:** Es werden keine Aktionen gestartet.
- **Benachrichtigung senden:** Es wird eine Benachrichtigung an den Administrator gesendet, die ihm mitteilt, dass der Schwellenwert erreicht wurde.
- **Älteste Protokolldateien löschen:** Die ältesten Protokolldateien werden automatisch gelöscht bis die Datenmenge entweder unterhalb des eingestellten Schwellenwerts liegt oder die Protokoll-Partition leer ist. Zusätzlich erhält der Administrator eine Benachrichtigung über das Ereignis.
- **System herunterfahren:** Das System fährt automatisch herunter.Der Administrator erhält eine Benachrichtigung über das Ereignis.
  Falls das System heruntergefahren wird, muss der Administrator die Konfiguration für die lokale Protokollierung ändern, die Löschung von Protokolldateien konfigurieren oder Protokolldateien manuell verschieben beziehungsweise löschen. Wenn die Ursache für das Herunterfahren des Systems weiterhin besteht, wird sich das System wieder herunterfahren, sobald der Prozess der Protokollüberprüfung das nächste Mal läuft. Dieser Prozess findet täglich um 0.00 Uhr statt.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

17.11.2 Remote-Syslog-Server

Auf der Registerkarte *Protokolle & Berichte* > *Protokolleinstellungen* > *Remote-Syslog-Server* werden die Einstellungen für die entfernte Protokollierung vorgenommen. Diese Funktion ermöglicht es, Protokollmeldungen von der UTM an andere Hosts weiterzuleiten. Das ist

insbesondere in Netzwerken nützlich, die einen dedizierten Host besitzen, der die Protokollinformationen von mehreren UTM sammelt. Auf dem ausgewählten Host muss in diesem Fall ein Protokollierungs-Daemon in Betrieb sein, der mit dem Syslog-Protokoll kompatibel ist.

Um einen Remote-Syslog-Server zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie Remote-Syslog auf der Registerkarte *Remote-Syslog-Server*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Remote-Syslog-Einstellungen* kann nun bearbeitet werden.

2. **Klicken Sie auf das Plussymbol im Feld *Syslog-Server*, um einen Server anzulegen.**
   Das Dialogfenster *Syslog-Server hinzufügen* wird geöffnet.

3. **Nehmen Sie die folgenden Einstellungen vor:**
   Name: Geben Sie einen aussagekräftigen Namen für den Remote-Syslog-Server ein.

   Server: Wählen Sie den Host oder fügen Sie einen Host hinzu, der die Protokolldaten von der UTM entgegennehmen soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

   > **Warnung –** Wählen Sie keine Netzwerkschnittstelle der UTM aus, um sie als Remote-Syslog-Host zu verwenden – das würde zu einer Protokollierungsschleife führen.

   Port: Wählen Sie eine Dienstdefinition oder fügen Sie eine Dienstdefinition hinzu, die für die Verbindung verwendet werden soll. Das Hinzufügen einer Definition wird auf der Seite *Definitionen & Benutzer > Netzwerkdefinitionen > Netzwerkdefinitionen* erläutert.

4. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Remote-Syslog-Puffer

In diesem Abschnitt können Sie die Puffergröße des Remote-Syslogs ändern. Die Puffergröße ist die Anzahl der Protokollzeilen, die im Puffer vorgehalten werden. Der Standardwert ist 1000. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Remote-Syslog-Protokollauswahl

Dieser Abschnitt kann nur bearbeitet werden, wenn Remote-Syslog aktiviert ist. Markieren Sie die Auswahlkästchen von den Protokollen, die an den Syslog-Server geschickt werden sollen.

Über die Option *Alle auswählen* können Sie alle Protokolle auf einmal auswählen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

17.11.3 Ausgelagerte Protokollarchive

Auf der Registerkarte *Protokolle & Berichte > Protokolleinstellungen > Ausgelagerte Protokollarchive* werden die Einstellungen für eine ausgelagerte Archivierung der Protokolldaten vorgenommen. Wenn die ausgelagerte Protokolldatei-Archivierung aktiviert ist, werden die Protokolldateien des Vortages in einer Datei zusammengepackt und komprimiert und dann an den entfernten Protokollarchiv-Host gesendet. Über die Auswahlliste können Sie Ihre bevorzugte Übertragungsmethode wählen.

Um ein ausgelagertes Protokollarchiv zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die Funktion *Ausgelagerte Protokollarchive*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Abschnitt *Ausgelagertes Protokollarchiv* kann nun bearbeitet werden.

2. **Wählen Sie die Archivierungsmethode.**
   Wählen Sie aus der Auswahlliste Ihre bevorzugte Archivierungsmethode aus. Abhängig von Ihrer Wahl werden unten die zugehörigen Konfigurationsoptionen angezeigt. Sie können zwischen den folgenden Archivierungsmethoden wählen:

   - **FTP-Server:** Für das *File Transfer Protocol* (FTP, Dateiübertragungsprotokoll) müssen die folgenden Parameter gesetzt werden:
     - **Host:** Hostdefinition für den FTP-Server.
     - **Dienst:**TCP-Port, auf dem der Server lauscht.
     - **Benutzername:** Tragen Sie den Benutzernamen für das FTP-Serverkonto ein.
     - **Kennwort:** Tragen Sie das Kennwort für das FTP-Serverkonto ein.
     - **Pfad:** Tragen Sie den relativen Pfad zum FTP-Server sein.
   - **SMB-(CIFS)-Freigabe:** Für die SMB-Methode müssen die folgenden Parameter gesetzt werden:
     - **Host:** Wählen Sie die Hostdefinition für den SMB-Server aus.
     - **Benutzername:** Tragen Sie den Benutzernamen für das SMB-Konto ein.

- **Kennwort:** Tragen Sie das Kennwort für das SMB-Konto ein.

  Sicherheitshinweis – Das Kennwort wird in Klartext in der Konfigurationsdatei gespeichert. Daher wird empfohlen, eine Benutzer-/Kennwortkombination anzulegen, die ausschließlich für Protokollierungszwecke verwendet wird.

- **Freigabe:** SMB-Freigabename.Geben Sie den Pfad oder die Informationen zum freigegebenen Netzwerk ein, an das die Protokolldateien übertragen werden, z. B. `/logs/log_file_archive`.
- **Arbeitsgruppe/Domäne:** Geben Sie die Arbeitsgruppe oder Domäne an, zu der das Protokollarchiv gehört.

- **Secure Copy (SSH-Server):** Für die SCP-Methode muss der öffentliche SSH-DSA-Schlüssel zu den autorisierten Schlüsseln des SCP-Servers hinzugefügt werden. In einem Linux-System können Sie den SSH-DSA-Schlüssel einfach über die Zwischenablage in die Datei `~/.ssh/authorized_keys` des dafür konfigurierten Benutzerkontos kopieren. Während der Installation erzeugt Sophos UTM einen neuen SSH-DSA-Schlüssel. Aus Sicherheitsgründen wird der SSH-DSA-Schlüssel nicht in Backups gespeichert. Nach einer Neuinstallation oder der Installation eines Backups müssen Sie daher den neuen SSH-DSA-Schüssel auf den entfernten Server kopieren, damit die Protokolldateiarchive auf den SCP-Server kopiert werden können.
  Für die SCP-Methode müssen die folgenden Einstellungen vorgenommen werden:
  - **Host:** Wählen Sie die Hostdefinition für den SCP-Server aus.
  - **Benutzername:** Tragen Sie den Benutzernamen für das SCP-Serverkonto ein.
  - **Pfad:** Tragen Sie den vollständigen Pfad ein, in dem die Protokolldateien gespeichert werden sollen.
  - **Öffentlicher DSA-Schlüssel:** Fügen Sie den öffentlichen DSA-Schlüssel zur Liste der autorisierten Schlüssel auf dem entfernten Speicher-Rechner hinzu.
- **Per E-Mail senden:** Damit die Protokollarchive per E-Mail versendet werden, geben Sie eine gültige E-Mail-Adresse ein.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Wenn die Datenübertragung fehlschlägt, verbleibt die Archivdatei auf der UTM. Die UTM versucht bei jeder Protokollüberprüfung, alle verbliebenen Archivdateien zu übertragen.

17.12 Berichteinstellungen

Im Menü *Protokolle & Berichte > Berichtseinstellungen* können Sie die Einstellungen für Berichtsfunktionen vornehmen, wie das Ein- und Ausschalten bestimmter Berichtsfunktionen, das Bestimmen von Zeiträumen und der Menge zu speichernder Daten. Des Weiteren können Sie Daten anonymisieren, um den Datenschutz zu verbessern.

17.12.1 Einstellungen

Die Registerkarte *Einstellungen* ermöglicht Ihnen, den Umgang mit Berichtsdaten zu regeln und festzulegen, wie lange Berichtsdaten auf dem System gespeichert werden, bevor sie automatisch gelöscht werden. Einstellungen für die folgenden Themenbereiche können vorgenommen werden:

- Application Control
- Authentifizierung
- Email Protection
- Firewall
- IPS
- Netzwerknutzung
- Fernzugriff
- Web Protection
- Webserver Protection

Verwenden Sie die Auswahlkästchen auf der linken Seite, um die Berichtsfunktion für einen bestimmten Themenbereich ein- oder auszuschalten. Standardmäßig ist die Berichtsfunktion für alle Themenbereiche eingeschaltet.

Verwenden Sie die Auswahllisten auf der rechten Seite, um festzulegen, wie lange die Berichtsdaten aufbewahrt werden sollen.

Hinweis – Das Ausschalten unnötiger Berichtsfunktionen senkt die Grundlast des Systems und reduziert Leistungsengpässe. Versuchen Sie, die Zeiträume so kurz wie möglich zu halten, da große Mengen gespeicherter Daten eine höhere Grundlast für das System bedeuten und längere Antwortzeiten auf den dynamischen Berichtsseiten verursachen.

Die Einstellungen auf dieser Registerkarte wirken sich nicht auf die Protokolldateiarchive aus.

Detailgrad der Web-Protection-Berichte

In diesem Bereich können Sie den Detailgrad für Ihre Web-Protection-Berichte festlegen. Beachten Sie, dass ein höherer Detailgrad eine spürbare Erhöhung der Speicherauslastung und Systemlast verursacht, deshalb sollten Sie den Detailgrad nur erhöhen, wenn es notwendig ist.

Die folgenden Detailgrade sind verfügbar:

- **Nur Domäne:** Die Berichte zeigen die Top-Level-Domäne und die Second-Level-Domäne einer URL an, z. B. `beispiel.de`.Third-Level-Domänen werden angezeigt, wenn sie erzwungen sind, z. B. `example.co.uk`.
- **Komplette Domäne:** Die Berichte zeigen die komplette Domäne an, z. B. `www.beispiel.de` oder `shop.beispiel.de`
- **1 URL-Ebene:** Die Berichte zeigen zusätzlich das erste (virtuelle) Verzeichnis einer URL an, z. B. `www.beispiel.de/de/`.
- **2 URL-Ebenen:** Die Berichte zeigen zusätzlich die ersten beiden (virtuellen) Verzeichnisse einer URL an, z. B. `www.beispiel.de/de/produkte/`.
- **3 URL-Ebenen:** Die Berichte zeigen zusätzlich die ersten drei (virtuellen) Verzeichnisse einer URL an, z. B. `www.beispiel.de/de/produkte/neu/`.

Einstellungen für Gesamtbericht

In diesem Abschnitt können Sie jeweils die Anzahl an Gesamtberichten festlegen, die aufbewahrt werden soll:

- Tägliche Berichte: Maximal 60
- Wöchentliche Berichte: Maximal 52
- Monatliche Berichte: Maximal 12

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Weitere Informationen zum Gesamtbericht und seinen Optionen finden Sie unter *Protokolle & Berichte* > *Gesamtbericht*.

PDF-Papiereinstellungen

Das voreingestellte Papierformat für den PDF-Gesamtbericht ist A4.Sie können die Auswahlliste verwenden, um alternativ *Letter* oder *Legal* zu wählen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Fernzugriffs-Nutzungsstatistik

Hier können Sie die Erfassung von Nutzungsdaten über Fernzugriffsverbindungen aktivieren und deaktivieren. Ist die Option ausgewählt, werden Daten über Fernzugriffsverbindungen gespeichert und auf der Registerkarte *Protokolle & Berichte > Fernzugriff > Sitzung* in den Spalten *Hoch* und *Herunter* angezeigt. Ist die Option deaktiviert, werden keine entsprechenden Daten erfasst. Beachten Sie, dass sich die Systemlast erhöhen kann, wenn die Option aktiv ist.

Einstellungen für CSV-Trennzeichen

An dieser Stelle können Sie festlegen, welches Trennzeichen beim Export von Berichtsdaten in das CSV-Format verwendet wird. Beachten Sie, dass unter Windows das Trennzeichen mit den regionalen Einstellungen Ihres Systems übereinstimmen sollte, damit die exportierten Daten korrekt in einem Tabellenkalkulationsprogramm wie beispielsweise Excel angezeigt werden.

IPFIX-Accounting

Mithilfe von IPFIX lassen sich Informationen zum IPv4-Datenfluss der UTM an den Dienstanbieter weiterleiten, z. B. zwecks Überwachung, Berichterstattung, Accounting und Rechnungsstellung.

Bei IPFIX (Internet Protocol Flow Information Export) handelt es sich um ein nachrichtenbasiertes Protokoll für den universellen Export von Netzwerkverkehrsinformationen. Die Netzwerkverkehrsinformationen werden zunächst von einem *exporter* gesammelt und anschließend zu einem *collector* weitergesendet. Typische Netzwerkverkehrsinformationen des IPv4-Datenflusses sind *Quell- und Zieladresse, Quell- und Zielport, Byte, Pakete und Klassifizierungsdaten des Netzwerkverkehrs*.

Bei Aktivierung dieser Funktion exportiert die UTM die IPFIX-Accounting-Daten. Der collector befindet sich im Allgemeinen bei einem Dienstanbieter, der die Netzwerkverkehrsdaten einer oder mehrerer Ihrer UTMs sammelt und analysiert. Während der Systemkonfiguration bei Ihrem Dienstanbieter erhalten Sie den Hostnamen, und Sie müssen pro exporter, also pro

UTM, eine OID (Observation Domain ID) festlegen. Geben Sie diese Daten in die entsprechenden Felder ein.

Der Datenexport erfolgt über den UDP-Port 4739. Eine einzelne Netzwerkverbindung nutzt zwei IPFIX-Datenströme – einen für den Export, den anderen für die Antwort.

Sicherheitshinweis – Beachten Sie, dass die Netzwerkverkehrsdaten bei IPFIX unverschlüsselt übertragen werden. Deshalb wird empfohlen, die Daten lediglich über private Netzwerke zu versenden.

Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

17.12.2 Ausnahmen

Auf der Registerkarte *Berichteinstellungen* > *Ausnahmen* können Sie bestimmte Domänen und Adressen von der Berichterstellung ausnehmen. Das betrifft sowohl den Gesamtbericht als auch die jeweiligen Abschnitte des Menüs *Protokolle & Berichte* und die entsprechenden statistischen Informationen.

Hinweis – Vorgenommene Änderungen sind nicht umgehend auf den Seiten für die Tagesstatistik sichtbar, da die Aktualisierung nur alle 10 bis 15 Minuten vorgenommen wird. Beachten Sie außerdem die Import-Funktion, mit der Sie mehrere Einträge auf einmal definieren können.

Berichtsausnahmen: Web

In diesem Abschnitt können Sie die Domänen festlegen, die von den Web-Protection-Berichten ausgenommen werden. Die Domänennamen müssen genau so eingegeben werden, wie sie im Bericht *Domänen* auf der Registerkarte *Protokolle & Berichte* > *Web Protection* > *Internetnutzung* aufgelistet sind. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Berichtsausnahmen: Mail

In diesen beiden Abschnitten können Sie Domänen und E-Mail-Adressen festlegen, die von allen Email-Protection-Berichten ausgenommen werden,

Über das Feld *Domänen* lassen sich alle E-Mail-Adressen einer bestimmten Domäne ausschließen. Geben Sie lediglich den Teil der E-Mail-Adresse an, der die Domäne beschriebt, z. B. `sophos.com`. Über das Feld *Adressen* lassen sich bestimmte E-Mail-Adressen von den Berichten ausschließen. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

E-Mails mit den festgelegten Domänennamen oder Adressen als Sender oder Empfänger werden von den Email-Protection-Berichten ausgenommen.

Berichtsausnahmen: Network Protection

In diesem Abschnitt können Sie die IPv4- und IPv6-Adressen festlegen, die von den Network-Protection-Berichten ausgenommen werden. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

Berichtsausnahmen: Netzwerkverkehr

In diesem Abschnitt können Sie IPv4- und IPv6-Adressen festlegen, die von allen Netzwerknutzungsberichten ausgenommen werden. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu speichern.

17.12.3 Anonymisierung

Die Registerkarte *Berichtseinstellungen* > *Anonymisierung* ermöglicht Ihnen, Daten – basierend auf dem Vier-Augen-Prinzip – zu anonymisieren. Das bedeutet, dass eine Entanonymisierung nur möglich ist, wenn zwei verschiedene Leute dieses Vorgehen beschließen. Anonymisierung stellt sicher, dass Benutzerdaten geheim bleiben, wenn Protokoll- und Berichtsdaten eingesehen werden. Dadurch können Aktionen (z. B. Surfverhalten) nicht auf eine bestimmte Person zurückverfolgt werden.

Um Anonymisierung zu verwenden, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die Anonymisierung auf der Registerkarte *Anonymisierung*.**
   Klicken Sie auf den Schieberegler.

   Der Schieberegler wird gelb und der Bereich *Anonymisierungs-Einstellungen* kann bearbeitet werden.

2. **Geben Sie zwei Sicherheitskennwörter ein.**
   Das Vier-Augen-Prinzip ist nur gewährleistet, wenn zwei verschiedene Personen ein Kennwort eingeben, das der jeweils anderen Person unbekannt ist.

3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Um Anonymisierung (global) wieder zu deaktivieren, sind beide Kennwörter erforderlich.

1. **Klicken Sie auf der Registerkarte *Anonymisierung* auf den Schieberegler.**
   Der Schieberegler wird gelb und der Bereich *Anonymisierungs-Einstellungen* kann bearbeitet werden.
2. **Geben Sie beide Kennwörter ein.**
   Geben Sie das erste und das zweite Kennwort ein, die zur Aktivierung der Anonymisierung angegeben wurden.
3. **Klicken Sie auf *Übernehmen*.**
   Ihre Einstellungen werden gespeichert.

Falls nötig, kann die Anonymisierung für einzelne Benutzer aufgehoben werden. Weitere Informationen hierzu finden Sie unter *Protokolle & Berichte* > Web Protection und *Protokolle & Berichte* > Email Protection.

18 Support

Dieses Kapitel beschreibt die Support-Tools, die für die Sophos UTM zur Verfügung stehen.

Die Seiten des Menüs *Support* enthalten viele Funktionen, die den Benutzer unterstützen, von Weblinks über Kontaktinformationen bis hin zu nützlichen Netzwerk-Tools zur Bestimmung wichtiger Netzwerkeigenschaften, ohne dass auf die Kommandozeilen-Schnittstelle der UTM zugegriffen werden muss.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Dokumentation
- Druckbare Konfiguration
- Support kontaktieren
- Tools
- Erweitert

Darüber hinaus enthält die Hauptseite des Menüs *Support* Weblinks zu den folgenden Ressourcen:

- **Wissensdatenbank**: Die offizielle Wissensdatenbank von Sophos NSG stellt zahlreiche Informationen zur Konfiguration von Sophos UTM bereit.
- **Liste bekannter Probleme**: Die beschriebenen Probleme können entweder nicht behoben werden oder es sind Workarounds verfügbar, die zur Lösung führen.
- **Hardwarekompatibilität**: Eine Liste mit kompatibler Hardware für Sophos UTM.
- **Up2Date-Informationen:** Sophos NSG Up2Date-Blog informiert über Produktentwicklungen und Firmware-Updates.

18.1 Dokumentation

Onlinehilfe

Dieser Abschnitt beschreibt, wie Sie die Onlinehilfe öffnen und nutzen.

Handbuch herunterladen

Sie können das aktuelle Administratorhandbuch im PDF-Format herunterladen.Wählen Sie die Sprache des Handbuchs aus und klicken Sie auf *Herunterladen*. Um die PDF-Datei zu öffnen, benötigen Sie ein spezielles Programm wie Adobe Reader oder Xpdf.

Querverweis – Administrationshandbücher früherer UTM-Versionen und andere Dokumentationen können Sie von der Sophos-Knowledgebase herunterladen.

18.2 Druckbare Konfiguration

Auf der Seite *Support > Druckbare Konfiguration* können Sie einen detaillierten Bericht der aktuellen WebAdmin-Konfiguration erzeugen.

Hinweis – Die druckbare Konfiguration wird in einem neuen Fenster geöffnet. Je nach Browser kann es nötig sein, Pop-up-Fenster für WebAdmin zu erlauben.

Die Gliederung der druckbaren Konfiguration entspricht der Menüstruktur von WebAdmin, um das Auffinden der entsprechenden Konfigurationsoptionen im WebAdmin zu erleichtern.

Die Browser-Seite der druckbaren Konfiguration besteht aus einer Übersichtsseite, genannt *Index*, und mehreren Unterseiten. Links zu Unterseiten sind blau hervorgehoben. Unterseiten enthalten detaillierte Informationen zu dem jeweiligen Thema. Durch einen Klick auf den Link *Back to the index* unten auf einer Unterseite können Sie jederzeit von einer Unterseite zum Index zurückkehren.

Es gibt zwei weitere Ansichtsoptionen für die druckbare Konfiguration:

- WebAdmin format (WebAdmin-Format)
- Confd format (Confd-Format)

Die Links zu diesen Ansichtsoptionen finden Sie unten auf der Indexseite.

18.3 Support kontaktieren

Sophosbietet für seine Sicherheitslösungen umfangreichen Kundensupport an. Je nach Support-/Wartungsvertrag gibt es verschiedene Kategorien. Diese unterscheiden sich hinsichtlich

der Art des Kontakts zum Support und der zugesicherten Reaktionszeit durch die Sophos-Service-Abteilung und/oder Sophos NSG-zertifizierte Partner.

Alle Supportfälle, die Sophos UTM betreffen, werden über das MyUTM-Portal abgewickelt. Sie können über das Webformular einen Supportfall öffnen, indem Sie auf die Schaltfläche *Support-Ticket in neuem Fenster öffnen* klicken. Weitere Informationen finden Sie im MyUTM-Benutzerhandbuch.

18.4 Tools

Die Registerkarten des Menüs *Support* > *Tools* enthalten nützliche Netzwerk-Tools, mit denen wichtige Netzwerkeigenschaften ermittelt werden können, ohne dass auf die Kommandozeilen-Schnittstelle der UTM zugegriffen werden muss. Die Ausgabe der folgenden Tools kann eingesehen werden:

- Ping-Prüfung
- Traceroute
- DNS-Lookup

18.4.1 Ping-Prüfung

Das Programm *Ping* ist ein Computer-Netzwerk-Tool, mit dem man testen kann, ob ein bestimmter Host über ein IP-Netzwerk erreichbar ist. Ping sendet ICMP-*Echo-Anfrage*-Pakete an den Zielhost und lauscht auf Antworten in Form von ICMP-*Echo-Antwort*-Paketen. Aus Zeitintervallen und Antworthäufigkeiten schätzt Ping die Dauer des Paketumlaufs und die Paketverlustrate zwischen den Hosts.

Um eine Ping-Prüfung durchzuführen, gehen Sie folgendermaßen vor:

1. **Wählen Sie den Ping-Host.**
   Wählen Sie den Host, den Sie „anpingen“ möchten. Im Feld *Ping-Host* können Sie einen Host auswählen, für den eine Hostdefinition existiert. Alternativ können Sie auch *Benutzerdefinierte(r) Hostname/IP-Adresse* wählen und im Feld darunter einen benutzerdefinierten Hostnamen oder eine benutzerdefinierte IP-Adresse angeben.

2. **Wählen Sie die IP- Version** (nur verfügbar, wenn IPv6 global aktiv ist).
   Wählen Sie in der Auswahlliste *IP-Version* einen der Einträge *IPv4* oder *IPv6*.

3. **Klicken Sie auf *Übernehmen*.**
   Die Ausgabe der Ping-Prüfung wird im Abschnitt *Ping-Prüfungsergebnis* angezeigt.

18.4.2 Traceroute

Das Programm *Traceroute* ist ein Computer-Netzwerk-Tool zur Bestimmung der Route, die von Paketen in einem IP-Netzwerk genommen wird. Es listet die IP-Adressen der Router auf, über die das versendete Paket transportiert wurde. Sollte der Pfad der Datenpakete kurzfristig nicht bestimmbar sein, wird ein Stern (*) an Stelle der IP-Adresse angezeigt. Nach einer bestimmten Zahl an Fehlversuchen wird die Überprüfung abgebrochen. Der Abbruch einer Überprüfung kann viele Gründe haben, der wahrscheinlichste ist jedoch, dass eine Firewall im Netzwerkpfad Traceroute-Pakete blockiert.

Um eine Route nachzuvollziehen, gehen Sie folgendermaßen vor:

1. **Legen Sie den Traceroute-Host fest.**
   Wählen Sie den Host, für den Sie die Route bestimmen wollen. Im Feld *Traceroute-Host* können Sie einen Host auswählen, für den eine Hostdefinition existiert. Alternativ können Sie auch *Benutzerdefinierte(r) Hostname/IP-Adresse* wählen und im Feld darunter einen benutzerdefinierten Hostnamen oder eine benutzerdefinierte IP-Adresse angeben.

2. **Wählen Sie die IP- Version** (nur verfügbar, wenn IPv6 global aktiv ist).
   Wählen Sie in der Auswahlliste *IP-Version* einen der Einträge *IPv4* oder *IPv6*.

3. **Hop-Adressen (Abschnitte) numerisch statt symbolisch und numerisch ausgeben** (optional).
   Wenn Sie diese Option wählen, wird für jedes Gateway im Pfad eine Adresse-zu-Name-Auflösung durch einen Namensserver durchgeführt und gespeichert.

4. **Klicken Sie auf *Übernehmen*.**
   Die Ausgabe von Traceroute wird im Abschnitt *Traceroute-Ergebnis* angezeigt.

18.4.3 DNS-Lookup

Das Programm *host* ist ein Netzwerk-Tool zur Abfrage von DNS-Namensservern. Es führt DNS-Lookups durch und zeigt die Antworten an, die von den befragten Namensservern zurückkommen.

Um ein DNS-Lookup durchzuführen, gehen Sie folgendermaßen vor:

1. **Geben Sie den Hostnamen oder die IP-Adresse ein.**
   Geben Sie den Hostnamen oder die IP-Adresse eines Hosts ein, für den Sie DNS-Informationen erhalten wollen.
2. **Wählen Sie *Ausführliche Ausgabe aktivieren*** (optional).
   Wählen Sie diese Option, damit in der Ausgabe ausführlichere Informationen auftauchen.
3. **Klicken Sie auf *Übernehmen*.**
   Die Ausgabe von dig wird im Abschnitt *DNS-Suchergebnis* angezeigt.

18.5 Erweitert

Das Menü *Support* > *Erweitert* bietet weitere Informationen zu Ihrer UTM und gewährt Zugriff auf erweiterte Funktionen. Es bietet einen Überblick über laufende Prozesse und lokale Netzwerkverbindungen und Sie erhalten Einblick in die Routing-Tabelle und die Netzwerkschnittstellen-Tabelle. Darüber hinaus können Sie ein Support-Paket herunterladen, das Ihnen bei der Fehlersuche und Wiederherstellung hilft sowie Hintergrundinformationen zu internen Konfigurationsreferenzen bietet, welche Ihnen in Protokolldateien begegnen können.

18.5.1 Prozesse

Das Programm *ps* stellt eine Kopfzeile dar gefolgt von Zeilen, die Informationen über die laufenden Prozesse auf dem System enthalten. Diese Informationen sind nach ihrem „Controlling Terminal“ (dt. Steuerkonsole) und dann nach ihrer Prozess-ID sortiert.

18.5.2 LAN-Verbindungen

Das Programm *netstat* (Abkürzung für *Network Statistics*, dt. Netzwerkstatistiken) ist ein Netzwerk-Tool, das alle augenblicklich aktiven, sowohl eingehenden als auch ausgehenden, Internetverbindungen eines Computers anzeigt.

18.5.3 Routen

Das Programm *ip* ist ein Netzwerk-Tool, das zur Kontrolle des TCP/IP-Netzwerk- und Datenverkehrs dient. Mit dem Parameter `route show table all` werden die Inhalte aller Routing-Tabellen der UTM angezeigt.

18.5.4 Schnittstellen

Die Tabelle zeigt alle konfigurierten Schnittstellen von Sophos UTM, sowohl Netzwerkkarten als auch virtuelle Schnittstellen. Die Daten werden vom Programm *ip* durch den Parameter `addr` erzeugt. Schnittstellen und deren Eigenschaften werden angezeigt.

18.5.5 Konfigurations-Abbild

Für die Fehlersuche und für Wiederherstellungszwecke ist es nützlich, über die Installation von Sophos UTM so viele Informationen wie möglich zu sammeln. Auf der Registerkarte *Support > Erweitert > Konfigurations-Abbild* kann das Support-Paket heruntergeladen werden, das genau diese Funktion bietet. Die `zip`-Datei enthält Folgendes:

- Das komplette Abbild der UTM-Konfiguration (`storage.abf`). Beachten Sie, dass es sich dabei nicht um eine echte Backup-Datei handelt – einige Informationen, z. B. die Kennwörter, sind nicht in dieser Datei enthalten. Sie kann daher nur zur Fehlerbehebung genutzt werden.
- Informationen über die gegenwärtig genutzte Hardware (`hwinfo`).
- Informationen über die installierten Software-Pakete (`swinfo`).

18.5.6 REF auflösen

Zur Fehlerbehebung können vom System genutzte Configuration References (Konfigurationsreferenzen) aufgelöst werden. Wenn Sie irgendwo in den Protokollen (Logs) auf solche References stoßen, können Sie die Zeichenfolge (z. B. `REF_DefaultSuperAdmin`) in das Eingabefeld kopieren. Auf der Registerkarte wird anschließend ein Auszug aus der Datenstruktur des Konfigurations-Daemons angezeigt.

19 Abmelden

Sie können sich von UTM durch einen Klick auf den Menüpunkt *Abmelden* abmelden. Wenn Sie sich nicht richtig vom WebAdmin abmelden oder der Browser mit einer offenen Sitzung geschlossen wird, kann es passieren, dass Sie sich für die folgenden 30 Sekunden nicht anmelden können.

Hinweis – Beachten Sie, dass Sie abgemeldet werden, wenn Sie während einer Sitzung zu einer anderen Internetseite wechseln. In diesem Fall müssen Sie sich neu anmelden.

20 Benutzerportal

Dieses Kapitel enthält Informationen über die Funktionsweise des Benutzerportals und die Dienste, die es den Endbenutzern bereitstellt.

Das Benutzerportal von Sophos UTM ist eine Browser-basierte Anwendung, die autorisierten Benutzern unter anderem personalisierte E-Mail-Dienste und Dienste für den Fernzugriff zur Verfügung stellt. Der Zugriff ist über die URL von Sophos UTM möglich, zum Beispiel `https://192.168.2.100` (beachten Sie das HTTPS-Protokoll).

Benutzer können auf der Anmeldeseite eine Sprache aus der Auswahlliste auswählen, die sich rechts in der Kopfleiste befindet.

Abhängig von den im WebAdmin vom Administrator aktivierten Diensten und Funktionen können Benutzer auf folgende Dienste zugreifen:

- Mail-Quarantäne
- Mail-Protokoll
- POP3-Konten
- Absender-Whitelist
- Absender-Blacklist
- Hotspots
- Client-Authentifizierung
- OTP-Token
- Fernzugriff
- HTML5-VPN-Portal
- Kennwort ändern
- HTTPS-Proxy

Wenn die Funktion für einmalige Kennwörter (OTP) aktiviert ist, wird nach dem Anmeldeversuch unter bestimmten Bedingungen eine Anmeldeseite mit einem oder mehreren QR-Codes angezeigt. Die Anmeldeseite wird nur dann angezeigt, wenn die Funktion *OTP-Token automatisch für Benutzer erstellen* aktiviert wurde und der Benutzer nur mit seinem benutzerspezifischen Kennwort angemeldet ist (d. h. kein einmaliges Kennwort wird angefügt) und für den Benutzer ein unbenutztes OTP-Token verfügbar ist. Auf der Seite werden

Anweisungen zur Konfiguration eines Mobilgeräts für die Generierung einmaliger Kennwörter angezeigt. Nach der Konfiguration des Mobilgeräts kann sich der Benutzer erneut anmelden. Dazu kann er jetzt das UTM Kennwort und direkt danach das einmalige Kennwort eingeben. Beispiel: Wenn Ihr UTM Kennwort `1z58.xa` ist und das einmalige Kennwort lautet `123456`, geben Sie zur Anmeldung `1z58.xa123456` ein.

20.1 Benutzerportal: Mail-Quarantäne

Auf dieser Registerkarte können Benutzer Nachrichten in Quarantäne anzeigen und gegebenenfalls freigeben.

Hinweis – Die Registerkarte *Mail-Quarantäne* wird angezeigt, wenn POP3 oder SMTP im WebAdmin aktiviert ist und der Benutzer für diese Dienste konfiguriert wurde. Erhält der Benutzer E-Mails sowohl über SMTP als auch über POP3, werden die Nachrichten auf zwei Registerkarten verteilt: *POP3-Quarantäne* und *SMTP-Quarantäne*, mit den gleichen Funktionen.

Die Registerkarte *Mail-Quarantäne* zeigt eine Übersicht aller E-Mails für den Benutzer an, außer jenen, die von Sophos UTM blockiert und unter Quarantäne gestellt wurden. Damit POP3-Quarantäne-E-Mails angezeigt werden, muss der Benutzer auf der Registerkarte *POP3-Konten* seine POP3-Zugangsdaten eingeben.

Quarantäne-E-Mails sortieren und filtern

Standardmäßig werden alle E-Mails angezeigt. Enthält die Liste mehr als zwanzig E-Mails, wird sie in mehrere Seiten unterteilt, durch die Sie mit den Schaltflächen Vorwärts (>) und Rückwärts (<) navigieren können.

Benutzer können die Anzeige anpassen:

> **Sortieren nach:** Standardmäßig wird die Liste nach Eingangsdatum sortiert. Nachrichten können nach Datum, Betreff, Absenderadresse und Nachrichtengröße sortiert werden.
>
> **und zeige:** Sie können wählen, ob 20, 50, 100, 250, 500 oder 1000 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Verschiedene Elemente auf der Seite ermöglichen das Filtern von E-Mails:

- **Anzahl der Nachrichten in Quarantäne:** Ganz oben auf der Seite befinden sich mehrere Auswahlkästchen, mit denen die E-Mail-Anzeige nach dem Grund für die Quarantäne (Schadsoftware, Spam, übereinstimmender Ausdruck, Dateierweiterung, MIME-Typ, unscannbar, andere) gefiltert werden kann.
- **Adressen** oder **Konten:** Ermöglicht es, Nachrichten nach Empfängeradresse (SMTP) oder Konto (POP3) zu filtern.
- **Abs./Empf./Betr.-Teilausdruck:** Hier können Benutzer einen Absender, Empfänger (nur mit POP3) oder Betreff eingeben, nach dem in den Quarantäne-Nachrichten gesucht werden soll.
- **Eingangsdatum:** Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Benutzer hier ein Datum ein oder wählen ein Datum über das Kalendersymbol.

Quarantäne-E-Mails verwalten

Benutzer können Aktionen für eine Nachricht mithilfe der Auswahlliste vor der Nachricht ausführen. Eine Aktion kann auch für mehrere ausgewählte Nachrichten durchgeführt werden. Verwenden Sie die Auswahlkästchen vor den Nachrichten oder klicken Sie auf Nachrichten, um sie auszuwählen. Wählen Sie dann eine der verfügbaren Aktionen in der Auswahlliste unter der Tabelle. Die folgenden Aktionen sind möglich:

- **Anzeigen** (nur für einzelne Meldungen verfügbar): Öffnet ein Fenster mit dem E-Mail-Inhalt.
- **Herunterladen:** Die gewählten Nachrichten werden im EML-Format heruntergeladen.
- **Löschen:** Die gewählten Nachrichten werden unwiderruflich gelöscht.
- **Absender auf Whitelist** (nur für einzelne Meldungen verfügbar): Verschiebt die E-Mail in Ihr Postfach und fügt den Absender zur Positivliste (Registerkarte *Absender-Whitelist*) hinzu. Nachfolgende E-Mails von diesem Absender werden nicht mehr unter Quarantäne gestellt. Beachten Sie, dass E-Mails mit schädlichem Inhalt immer unter Quarantäne gestellt werden, auch wenn der Absender auf der Whitelist steht.
- **Freigeben:** Die gewählten Nachrichten werden aus der Quarantäne freigegeben.
- **Freigeben und als Fehlfund melden:** Die gewählten Nachrichten werden aus der Quarantäne freigegeben und als Fehlfund (false positive) an das Spam-Scan-Programm gemeldet.

Hinweis – Welche Aktionen verfügbar sind, hängt vom Quarantänegrund und von den WebAdmin-Einstellungen ab. Benutzer können nur Nachrichten freigeben, für die sie explizit die Erlaubnis haben.Nur der Administrator kann *alle* Nachrichten aus der Quarantäne freigeben.

Globale Aufräumaktion wählen: Hier finden Sie einige Löschoptionen, die auf alle Nachrichten global angewendet werden, das heißt, unabhängig davon, ob sie ausgewählt sind und/oder angezeigt werden oder nicht.

20.2 Benutzerportal: Mail-Protokoll

Auf dieser Registerkarte können Endbenutzer ein Protokoll ihres über SMTP gesendeten E-Mail-Verkehrs anzeigen.

Hinweis – Die Registerkarte *Mail-Protokoll* führt nur E-Mail-Adressen der Domäne auf, die der SMTP-Proxy von Sophos UTM überwacht. Benutzer können die Registerkarte nur sehen, wenn ihnen der Administrator entsprechende Rechte zugewiesen hat.Wenn für einen Benutzer sowohl SMTP als auch POP3 aktiviert wurden, heißt diese Registerkarte *SMTP-Protokoll*.

Die Registerkarte *Mail-Protokoll* enthält Protokolleinträge über den gesamten E-Mail-Verkehr für alle E-Mail-Adressen des Benutzers. Für E-Mails, die nicht zugestellt werden konnten, enthalten die Protokolleinträge Informationen über die jeweilige Ursache. Durch einen Doppelklick auf einen Protokolleintrag wird ein Fenster mit weiterführenden Informationen angezeigt.

Standardmäßig werden alle E-Mails angezeigt. Enthält die Liste mehr als zwanzig E-Mails, wird sie in mehrere Seiten unterteilt, durch die Sie mit den Schaltflächen Vorwärts (>) und Rückwärts (<) navigieren können.

Benutzer können die Anzeige anpassen:

> **Sortieren nach:** Standardmäßig wird die Liste nach Eingangsdatum sortiert. Nachrichten können nach Datum, Betreff, Absenderadresse und Nachrichtengröße sortiert werden.

und zeige: Sie können wählen, ob 20, 50, 100, 250, 500 oder 1000 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Verschiedene Elemente auf der Seite ermöglichen das Filtern von E-Mails:

- **# Protokollereignisse in Datei:** Ganz oben auf der Seite befinden sich mehrere Auswahlfelder, mit denen E-Mails abhängig von ihrem Status eingeblendet und ausgeblendet werden können.
- **Adressen:** Ermöglicht es, E-Mails nach Absenderadresse zu filtern.
- **Abs./Betr.-Teilausdruck:** Hier können Benutzer einen Absender oder Betreff eingeben (oder einen Wortteil davon), nach dem in den Quarantäne-Nachrichten gesucht werden soll.
- **Eingangsdatum:** Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Benutzer hier ein Datum ein oder wählen ein Datum über das Kalendersymbol.

20.3 Benutzerportal: POP3-Konten

Auf dieser Registerkarte können sich Endbenutzer ausweisen, um ihre POP3-E-Mails in Quarantäne ansehen und freigeben und Quarantäneberichte erhalten zu können.

> **Hinweis –** Die Registerkarte *POP3-Konten* ist nur verfügbar, wenn der Administrator POP3 aktiviert und einen POP3-Server hinzugefügt hat.

Auf dieser Seite müssen Benutzer die Zugangsdaten zu den POP3-Konten eingeben, die sie benutzen. Es werden nur Spam-E-Mails, für die POP3-Kontozugangsdaten hinterlegt sind, im Benutzerportal angezeigt. Benutzer, für die POP3-Kontozugangsdaten gespeichert sind, erhalten einen eigenständigen Quarantänebericht für jede E-Mail-Adresse.

20.4 Benutzerportal: Absender-Whitelist

Auf dieser Registerkarte können Benutzer E-Mail-Absender auf die Positivliste (Whitelist) setzen, damit die Nachrichten dieser Absender niemals als Spam behandelt werden. E-Mails mit Viren oder unscannbare E-Mails werden jedoch stets unter Quarantäne gestellt.

Hinweis – Die Registerkarte *Absender-Whitelist* ist nur dann verfügbar, wenn die E-Mail-Adresse des Benutzers dem Netzwerk oder der Domäne angehört, die von Sophos UTM überwacht wird, und vom Administrator die Zugriffsrechte für diese Funktion gewährt wurden.

Absender können auf die Whitelist gesetzt werden, indem das Plussymbol angeklickt, eine Adresse eingegeben und auf das Häkchensymbol geklickt wird, um den Eintrag zu speichern. Benutzer können sowohl einzelne gültige E-Mail-Adressen (z. B. `mmustermann@beispiel.de`) als auch Adressen einer spezifischen Domäne eintragen, wobei ein Asterisk als Platzhalter dient (z. B. `*@beispiel.de`). Absender-Whitelist und Absender-Blacklist können gemeinsam verwendet werden: Der Benutzer kann zum Beispiel eine ganze Domäne (z. B. *@hotmail.com) auf die Blacklist setzen, während er einzelne E-Mail-Adressen dieser Domäne (z. B. `meinkollege@hotmail.com`) auf die Whitelist setzt und damit freigibt. Das funktioniert auch andersherum. Wenn genau dieselbe E-Mail-Adresse in beiden Listen vorhanden ist, gilt die Blacklist.

20.5 Benutzerportal: Absender-Blacklist

Auf dieser Registerkarte können Benutzer E-Mail-Absender auf die schwarze Liste (Blacklist) setzen, damit die Nachrichten dieser Absender immer als Spam behandelt werden.

Hinweis – Die Registerkarte *Absender-Blacklist* ist nur dann verfügbar, wenn die E-Mail-Adresse des Benutzers dem Netzwerk oder der Domäne angehört, die von Sophos UTM überwacht wird, und vom Administrator die Zugriffsrechte für diese Funktion gewährt wurden.

Die Blacklist wird sowohl auf SMTP- als auch auf POP3-E-Mails angewendet, wenn diese auf dem System aktiviert sind. Absender können auf die Blacklist gesetzt werden, indem man auf das Plussymbol klickt, die Adresse eingibt und zum Speichern auf das Häkchen klickt. Benutzer können sowohl einzelne gültige E-Mail-Adressen (z. B. `mmustermann@beispiel.de`) als auch Adressen einer spezifischen Domäne eintragen, wobei ein Asterisk als Platzhalter dient (z. B. `*@beispiel.de`). Absender-Whitelist und Absender-Blacklist können gemeinsam verwendet werden: Der Benutzer kann zum Beispiel eine ganze Domäne (z. B. *@hotmail.com) auf die Blacklist setzen, während er einzelne E-Mail-Adressen dieser Domäne (z. B. `meinkollege@hotmail.com`) auf die Whitelist setzt und damit freigibt. Das funktioniert auch

andersherum. Wenn genau dieselbe E-Mail-Adresse in beiden Listen vorhanden ist, gilt die Blacklist.

20.6 Benutzerportal: Hotspots

Die Hotspot-Funktion ermöglicht es, in Gaststätten, Hotels, Unternehmen usw. Gästen einen zeit- und volumenbeschränkten Internetzugang bereitzustellen.

Hinweis – Die Registerkarte *Hotspots* wird im Benutzerportal nur dann angezeigt, wenn der Administrator einen Hotspot vom Typ *Kennwort* oder *Voucher* erstellt hat und den betreffenden Benutzer in die Liste der zugelassenen Benutzer aufgenommen hat.

Auf dieser Registerkarte können Benutzer die Hotspot-Zugangsdaten an WLAN-Gäste verteilen. Welche Funktionen verfügbar sind, hängt von dem gewählten Hotspot-Typ ab: Entweder sie verteilen ein allgemeingültiges Kennwort oder Voucher.

Hotspot-Typ: Tages-Kennwort

Das Feld *Kennwort* enthält das aktuelle Kennwort. Dieses Kennwort wird einmal am Tag geändert. Benutzer haben aber auch die Möglichkeit, das Kennwort manuell zu ändern. Das vorhergehende Kennwort wird sofort ungültig. Alle laufenden Sitzungen werden beendet.

Um das Kennwort zu ändern, gehen Benutzer folgendermaßen vor:

1. **Sie öffnen im Benutzerportal die Registerkarte *Hotspots*.**
2. **Sie wählen einen Hotspot aus, dessen Zugangsinformationen sie bearbeiten möchten.**
   Sie wählen aus der Auswahlliste *Hotspot* den Hotspot aus, dessen Kennwort sie ändern möchten.
3. **Sie erstellen das neue Kennwort.**
   Dazu geben sie das neue Kennwort in das Feld *Kennwort* ein oder klicken auf die Schaltfläche *Erstellen*, um automatisch ein neues Kennwort zu erzeugen.
4. **Benutzer können die neuen Kennwörter per E-Mail versenden, indem sie das Auswahlkästchen *E-Mail senden* aktivieren.**

Das Kennwort wird an die vom Administrator spezifizierten E-Mail-Empfänger gesendet. Wenn der Administrator keine E-Mail-Adresse festgelegt hat, wird das Auswahlkästchen nicht angezeigt.

5. **Sie klicken auf *Speichern*.**
   Die Kennwortänderung tritt sofort in Kraft.

Hotspot-Typ: Voucher

Benutzer können Voucher mit einmaligen Zugangscodes erstellen. Sie können die Voucher drucken und ihren Gästen aushändigen. Die Liste der erstellten Voucher liefert einen Überblick über ihre Nutzung und erleichtert ihre Verwaltung.

Um Voucher zu erstellen, gehen Benutzer folgendermaßen vor:

1. **Sie öffnen im Benutzerportal die Registerkarte *Hotspots*.**

2. **Sie müssen die folgenden Einstellungen festlegen:**
   Hotspot: Sie müssen den Hotspot auswählen, für den sie einen Voucher erstellen möchten.

   Voucher-Definition: Der Administrator legt die verfügbaren Voucher-Typen fest. Das Unternehmen legt fest, welcher Voucher-Typ für welchen Zweck verwendet wird.

   Anzahl: Die Benutzer müssen angeben, wie viele Voucher dieses Typs erstellt werden sollen.

   Kommentar: Optional können sie Anmerkungen eingeben. Die Anmerkungen werden in der Voucher-Liste des Benutzers angezeigt.

   Druck: Benutzer können die Voucher auch sofort ausdrucken, indem sie diese Option auswählen.

   Seitenformat: Sie müssen das Seitenformat für den Druck auswählen.

   Voucher pro Seite: Sie legen fest, wie viele Voucher auf eine Seite gedruckt werden sollen.UTMrichtet die Voucher automatisch auf der Seite aus.

   QR-Code hinzufügen: Benutzer können festlegen, dass der gedruckte Voucher neben den Voucher-Textdaten auch einen QR-Code enthalten soll. Ein QR-Code ist ein quadratisches Bild, das codierte Daten enthält. Es lässt sich mit Mobilgeräten scannen, um die Hotspot-Anmeldeseite aufzurufen, auf der die Felder mit den erforderlichen Daten vorausgefüllt sind.

3. **Sie klicken auf die Schaltfläche *Voucher erstellen*.**
   Die Voucher werden generiert. Die Voucher werden sofort in der Voucher-Liste angezeigt. Jeder Voucher entspricht einer neuen Zeile. Wenn zuvor ausgewählt, werden die Voucher direkt ausgedruckt. Jeder Voucher hat einen einmaligen Code.

Hinweis – Inhalt, Größe und Layout der Voucher werden vom Administrator festgelegt.

In der Voucher-Liste können Benutzer die Voucher verwalten. Sie können die Liste sortieren und filtern, einen Kommentar eingeben oder ändern und sie können Voucher drucken, löschen oder exportieren.

- Zum Sortieren der Liste wählen sie in der Auswahlliste *Sortieren nach* ein Sortierkriterium aus. Mit der Auswahlliste auf der rechten Seite legen Benutzer fest, wie viele Voucher pro Seite angezeigt werden.
- Mit den Feldern *Status*, *Code* oder *Kommentar* kann die Liste gefiltert werden. Die Benutzer wählen das gewünschte Attribut aus oder geben es ein, um die Liste zu filtern. Die Liste wird bereits während der Eingabe gefiltert.Um den Filter zurückzusetzen, wählen sie den Statuseintrag *Alle* und löschen den eingegebenen Text in den Textfeldern *Code* bzw. *Kommentar*.
- Um einen Kommentar einzugeben oder zu bearbeiten, klicken sie in der *Kommentar*-Spalte des jeweiligen Vouchers auf das Notizbuch-Symbol. Ein Textfeld wird angezeigt. Benutzer können Text eingeben oder bearbeiten. Mit der Eingabetaste oder einem Klick auf das Häkchen werden die Änderungen gespeichert.
- Wenn sie Voucher drucken oder löschen möchten, aktivieren Benutzer das Auswahlkästchen vor den jeweiligen Vouchern und klicken unten auf die entsprechende Schaltfläche.

  Hinweis – Der Administrator kann festlegen, dass Voucher nach einem bestimmten Zeitraum automatisch gelöscht werden.

- Um Voucher zu exportieren, gehen Benutzer folgendermaßen vor: Sie aktivieren das Auswahlkästchen vor den jeweiligen Vouchern und klicken unterhalb der Liste auf die Schaltfläche *CSV exportieren*. In einem neu angezeigten Fenster können sie anschließend auswählen, ob die CSV-Datei gespeichert oder direkt geöffnet werden soll. Die ausgewählten Voucher werden gemeinsam in einer CSV-Datei gespeichert. Benutzer müssen beim Öffnen dieser Datei darauf achten, dass sie das korrekte Trennzeichen für die Spaltentrennung auswählen.

20.7 Benutzerportal: Client-Authentifizierung

Auf dieser Registerkarte können Endbenutzer die Setup-Datei des Sophos Authentication Agents (SAA) herunterladen. Der SAA kann als Authentifizierungsmethode für den Webfilter genutzt werden.

Hinweis – Die Registerkarte *Client-Authentifizierung* ist nur verfügbar, wenn Client-Authentifizierung vom Administrator aktiviert wurde.

20.8 Benutzerportal: OTP-Token

Auf dieser Registerkarte haben Endbenutzer Zugriff auf die QR-Codes und Daten für die Installation der OTP-Konfiguration auf ihren Mobilgeräten.

OTP-Token mit Google Authenticator konfigurieren

1. **Installieren Sie Google Authenticator auf Ihrem Mobilgerät.**
2. **Scannen Sie den QR-Code.**
3. **Öffnen Sie die App.**
   Sie zeigt das einmalige Kennwort an, das sich alle 30 Sekunden ändert.
4. **Öffnen Sie die Funktion, für die Sie das einmalige Kennwort nutzen möchten.**
   Der Administrator hat die Dienste konfiguriert, für die Sie das einmalige Kennwort eingeben müssen, zum Beispiel für eine Verbindung per Fernzugriff, für die Web Application Firewall oder für das Benutzerportal selbst.
5. **Geben Sie Ihren Benutzernamen und Ihr Kennwort für UTM ein und direkt danach das aktuelle einmalige Kennwort.Klicken Sie dann auf die Schaltfläche *Anmelden*.**
   Nun haben Sie Zugriff auf die Funktion.

Verwenden anderer Software

1. **Installieren Sie die Software auf Ihrem Mobilgerät.**
2. **Öffnen Sie die App.**
3. **Konfigurieren sie die App mithilfe der Daten neben dem QR-Code.**
   Die App generiert nun die einmaligen Kennwörter.
4. **Öffnen Sie die Funktion, für die Sie das einmalige Kennwort nutzen möchten.**
   Der Administrator hat die Dienste konfiguriert, für die Sie das einmalige Kennwort eingeben müssen, zum Beispiel für eine Verbindung per Fernzugriff, für die Web Application Firewall oder für das Benutzerportal selbst.
5. **Geben Sie Ihren Benutzernamen und Ihr Kennwort für UTM ein und direkt danach das aktuelle einmalige Kennwort.Klicken Sie dann auf die Schaltfläche *Anmelden*.**
   Nun haben Sie Zugriff auf die Funktion.

20.9 Benutzerportal: Fernzugriff

Auf dieser Registerkarte können Endbenutzer Client-Software für den Fernzugriff sowie für sie bereitgestellte Konfigurationsdateien herunterladen. Diese werden entsprechend den WebAdmin-Einstellungen des Administrators automatisch erstellt und bereitgestellt.

Hinweis – Die Registerkarte *Fernzugriff* ist nur zu sehen, wenn für den jeweiligen Benutzer der Fernzugriff aktiviert wurde.

Es sind jedoch nur jene Fernzugriffdaten für einen Benutzer verfügbar, die mit den Verbindungsarten übereinstimmen, die für ihn vom Administrator aktiviert wurden. Beispiel: Ein Benutzer, für den der SSL-VPN-Fernzugriff aktiviert ist, findet einen Abschnitt *SSL-VPN* vor.

Jede Verbindungsart wird in einem separaten Abschnitt angezeigt. Abhängig von der Verbindungsart sind Informationen und/oder Schaltflächen zum Herunterladen der entsprechenden Software verfügbar. Sofern zutreffend, finden Benutzer über den Abschnitten einen Link *Installationsanleitung in neuem Fenster öffnen*, über den sie eine detaillierte Installationsdokumentation öffnen können.

20.10 Benutzerportal: HTML5-VPN-Portal

Das HTML5-VPN-Portal ermöglicht Benutzern von externen Netzwerken aus den Zugriff auf interne Ressourcen über vorkonfigurierte Verbindungstypen und einen normalen Webbrowser.

Hinweis – Die Registerkarte *HTML5-VPN-Portal* wird ausschließlich Benutzern angezeigt, für die der Administrator VPN-Verbindungen eingerichtet hat und die zur Gruppe der zugelassenen Benutzer gehören.

Hinweis – Der Browser des Benutzers muss HTML5 unterstützen. Die folgenden Browser unterstützen die HTML5-VPN-Funktion: Firefox ab Version 6.0, Internet Explorer ab Version 10, Chrome, Safari ab Version 5 (nicht beim Betriebssystem Windows).

Auf der Registerkarte *HTML5-VPN-Portal* sind die zugelassenen Verbindungen aufgeführt. Die Symbole weisen auf den Verbindungstyp hin.

Um eine Verbindung zu verwenden, gehen Benutzer folgendermaßen vor:

1. **Sie klicken auf die jeweilige *Verbinden*-Schaltfläche.**
   Ein neues Browser-Fenster wird geöffnet. Inhalt und Aussehen dieses Fensters hängen vom Verbindungstyp ab. Wenn der Benutzer zum Beispiel eine HTTP- oder HTTPS-Verbindung aufgebaut hat, wird eine Website angezeigt. Bei SSH-Verbindungen wird eine Kommandozeile angezeigt.

2. **Im neuen VPN-Fenster arbeiten.**
   Für einige Aufgaben bietet das VPN-Fenster eine für den Verbindungstyp spezifische Menüleiste, die eingeblendet wird, wenn der Mauszeiger auf den oberen Rand des Fensters zeigt:

   - **Funktionstasten oder Tastenkombinationen verwenden:** Wenn Benutzer spezielle Befehle, wie Funktionstasten oder `STRG-ALT-ENTF` verwenden wollen, müssen sie den entsprechenden Eintrag im Menü *Keyboard* auswählen.

   - **Vom lokalen Rechner kopieren und in das VPN-Fenster einfügen:** Benutzer müssen auf dem lokalen Rechner den entsprechenden Text in die Zwischenablage kopieren. Im Verbindungsfenster müssen sie das *Clipboard*-Menü auswählen. Mit `STRG-V` fügen sie den Text in das Textfeld ein. Dann müssen sie

auf die Schaltfläche *Send to Server* klicken: Bei SSH- oder Telnet-Verbindungen wird der Text dann direkt an der Cursor-Position eingefügt. Bei RDP- oder VNC-Verbindungen wird der Text in die Zwischenablage des Servers kopiert und kann dann wie gewöhnlich eingefügt werden.

> **Hinweis –** Kopieren und Einfügen (Copy & Paste) ist bei Webapp-Verbindungen nicht möglich.

- **Im VPN-Fenster kopieren und in ein anderes Fenster einfügen:** Mit SSH- und Telnet-Verbindungen können Benutzer Texte wie bei lokalen Fenstern kopieren und einfügen. Bei RDP- und VNC-Verbindungen müssen die Benutzer im VPN-Fenster den entsprechenden Text in die Zwischenablage kopieren. Dann wählen sie das Menü *Clipboard*. Der kopierte Text wird im Textfeld angezeigt. Die Benutzer müssen den Text markieren und `STRG-C` drücken. Jetzt ist er in der lokalen Zwischenablage und kann wie gewöhnlich eingefügt werden.
- **Tastaturbelegung einer Remotedesktop-Verbindung ändern:** Benutzer können für Remotedesktop-Verbindungen mit einem Windows-Rechner die Tastatur-Spracheinstellung des VPN-Fensters ändern. Besonders für die Windows-Anmeldung gilt, dass die ausgewählte Sprache mit der Spracheinstellung in Windows übereinstimmen sollte, um eine korrekte Kennworteingabe zu ermöglichen. Die Benutzer müssen die gewünschte Sprache im Menü *Keyboard > Keyboard Layout* auswählen. Das ausgewählte Tastatur-Layout wird in einem Cookie gespeichert.
- **In einer Webapp-Verbindung zur Startseite zurückkehren:** Um zur Standardseite einer Webapp-Verbindung zurückzukehren, wählen Sie das Menü *Navigation > Home*.

3. **Nach getaner Arbeit wird die Verbindung geschlossen.**
   - Mit dem Befehl *Stop Session* im Menü *Connection* oder durch Schließen des Browser-Fensters (x-Symbol in der Titelleiste) wird die Verbindung geschlossen. Durch erneutes Anklicken der *Verbinden*-Schaltfläche wird eine neue Sitzung gestartet.
   - Mit dem Befehl *Suspend Session* im Menü *Connection* wird die Sitzung beendet. Der Sitzungsstatus wird für die Dauer von fünf Minuten gespeichert. Meldet sich der Benutzer während dieses Zeitraums wieder an, kann er die letzte Sitzung fortsetzen.

20.11 Benutzerportal: Kennwort ändern

Auf dieser Registerkarte können Endbenutzer ihr Kennwort für den Zugriff auf das Benutzerportal und, sofern verfügbar, für den Fernzugriff über PPTP ändern.

20.12 Benutzerportal: HTTPS-Proxy

Auf dieser Registerkarte können Benutzer das HTTP/S-Proxy-CA-Zertifikat importieren, damit keine Fehlermeldungen mehr angezeigt werden, wenn sie sichere Websites besuchen.

Hinweis – Die Registerkarte *HTTPS-Proxy* des Benutzerportals wird nur angezeigt, wenn der Administrator global ein HTTP/S-Proxy-Zertifikat bereitgestellt hat.

Nach Klicken auf die Schaltfläche *Proxy-CA-Zertifikat importieren* wird der Benutzer von seinem Browser gefragt, ob er der CA für verschiedene Zwecke vertraut.

Glossar

3

3DES
Triple Data Encryption Standard

A

ACC
Astaro Command Center

ACPI
Advanced Conguration and Power Interface

AD
Active Directory

Address Resolution Protocol
ARP ist ein Netzwerkprotokoll, das die Zuordnung von Netzwerkadressen (IP-Adressen) zu Hardwareadressen (MAC-Adressen) möglich macht.

ADSL
Asymmetric Digital Subscriber Line

Advanced Configuration and Power Interface
ACPI ist ein offener Industriestandard und stellt Schnittstellen zur Hardwareerkennung, Gerätekonfiguration und zum Energiemanagement von Computern zur Verfügung.

Advanced Programmable Interrupt Controller
APIC ist eine Architektur für die Verteilung von Interrupts in Multiprozessor-Computersystemen.

AES
Advanced Encryption Standard

AFC
Astaro Flow Classifier

AH
Authentication Header

AMG
Astaro Mail Gateway

APIC
Advanced Programmable Interrupt Controller

ARP
Address Resolution Protocol

AS
Autonomes System

ASCII
American Standard Code for Information Interchange

ASG
Astaro Security Gateway

Astaro Command Center
Software für die Überwachung und Verwaltung von mehreren Astaro Gateway-Produkten über eine einzige Software-Oberfläche. Seit Version 4 heißt die Software Sophos UTM Manger (SUM).

Astaro Security Gateway
Software für Unified Threat Management, die Mail- und Internetsicherheit umfasst. SPF ist eine Erweiterung des SMTP Protokolls

Authentication Header
AH ist ein IPsec-Protokoll und stellt die Authentizität der übertragenen Pakete sicher. Darüber hinaus schützt es gegen Replay-Angriffe.

Autonomes System
Ein AS ist ein IP-Netz, welches als Einheit verwaltet wird und ein gemeinsames (oder auch mehrere) interne Routing-Protokolle verwendet.

AWG
Astaro Web Gateway

AWS
Amazon Web Services

B

BATV
Bounce Address Tag Validation

BGP
Border Gateway Protocol

Bounce Address Tag Validation
BATV ist der Name einer Methode zur Bestimmung, ob die Antwort-Adresse einer E-Mail gültig ist. Es wurde entwickelt, um Bounce-Messages für gefälschte Antwort-Adressen zu verwerfen.

Broadcast
Ein Broadcast in einem Computernetzwerk ist eine Nachricht, bei der Datenpakete von einem Punkt aus an alle Teilnehmer eines Netzes übertragen werden. Zum Beispiel: Ein Netzwerk mit der IP-Adresse 192.168.2.0 und einer Netzmaske 255.255.255.0 hat die Broadcast-Adresse 192.168.2.255.

C

CA
Certificate Authority (Zertifizierungsinstanz)

CBC
Cipher Block Chaining

CDMA
Code Division Multiple Access

Certificate Authority (Zertifizierungsinstanz)
Eine CA (dt. Zertifizierungsinstanz) ist eine Entität oder Organisation, die digitale Zertifikate herausgibt.

CHAP
Challenge Handshake Authentication Protocol

Cipher Block Chaining
In der Kryptografie bezeichnet CBC eine Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten. Vor dem Verschlüsseln eines Klartextblocks wird dieser erst mit dem im letzten Schritt erzeugten Geheimtextblock per XOR (exklusives Oder) verknüpft.

Cluster
Gruppe von miteinander verbundenen Computern, die eng zusammen arbeiten, sodass sie in vielerlei Hinsicht wie ein einzelner Computer agieren.

CMS
Content Management System

CPU
Hauptprozessor

CRL
Certificate Revocation List (Zertifikatsperrliste)

CSS
Cascading Style Sheets

D

DC
Domänencontroller

DCC
Direct Client Connection

DDoS
Distributed Denial of Service

DER
Distinguished Encoding Rules

Destination Network Address Translation
DNAT ist ein spezieller Fall von NAT (Network Address Translation), bei dem die Zieladressinformationen in Datenpaketen durch andere ersetzt werden.

DHCP
Dynamic Host Configuration Protocol

Digital Signature Algorithm
DSA ist ein Standard der US-Regierung für digitale Signaturen.

Digital Subscriber Line
DSL ist eine Technologie zur digitalen Datenübertragung über herkömmliche Telefonleitungen.

Distinguished Encoding Rules
DER ist eine Methode zur Verschlüsselung von Datenobjekten (z.B. X.509-Zertifikate), um sie digital zu signieren oder um ihre Signatur zu überprüfen.

DKIM
DomainKeys Identified Mail

DMZ
Demilitarized Zone (Entmilitarisierte Zone)

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name Service

DOI
Domain of Interpretation

Domain Name Service
DNS ist ein hierarchisches System von Namen im Internet und dient zur Auflösung dieser Namen in IP-Adressen.

DoS
Denial of Service

DSA
Digital Signature Algorithm

DSCP
Differentiated Services Code Point

DSL
Digital Subscriber Line

DUID
DHCP Unique Identifier

Dynamic Host Configuration Protocol
DHCP ist ein Protokoll, das von Netzwerkgeräten verwendet wird, um IP-Adressen zu erhalten.

E

ECN
Explicit Congestion Notification

Encapsulating Security Payload
ESP ist ein IPsec-Protokoll, das für die Authentifizierung, Integrität und Vertraulichkeit von IP-Paketen sorgt.

ESP
Encapsulating Security Payload

Explicit Congestion Notification
ECN (Explicit Congestion Notification) ist eine Erweiterung des Internetprotokolls und ermöglicht End-to-End-Benachrichtigungen über Netzwerküberlastungen, ohne dass Pakete verworfen werden. ECN funktioniert nur, wenn beide Endpunkte einer Verbindung erfolgreich über die Verwendung verhandeln.

F

FAT
File Allocation Table

File Transfer Protocol
FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke.

FQHN
Fully Qualified Host Name

FTP
File Transfer Protocol

G

Generic Routing Encapsulation
GRE ist ein Netzwerkprotokoll und dient der Einkapselung von Datenpaketen in andere Protokolle, um sie in Form von IP-Tunneln zu transportieren.

GeoIP
Eine Technik, um den Standort von Geräten weltweit mit Hilfe von Satellitenbildern darzustellen.

Gerätebaum
Befindet sich unterhalb des Hauptmenüs und bietet Zugriff auf alle Gateway-Geräte, die mit dem SUM verbunden sind.

GRE
Generic Routing Encapsulation

GSM
Global System for Mobile Communications

H

H.323
H.323 ist ein Protokoll für die audiovisuelle Kommunikation über paketvermittelte Netzwerke.

HA
High Availabilty (Hochverfügbarkeit)

HCL
Hardware Compatibility List (Hardwarekompatibilitätsliste)

HELO
Ein Befehl im Simple Mail Transfer Protocol (SMTP), mit dem der Client auf den initialen Gruß des Servers antwortet.

High Availabilty (Hochverfügbarkeit)
Hochverfügbarkeit (High availability) bezeichnet die Fähigkeit eines Systems, bis zu einem gewissen Grad Ausfallsicherheit gewährleisten zu können.

HIPS
Host-based Intrusion Prevention System

HMAC
Hash-based Message Authentication Code

HTML
Hypertext Transfer Markup Language

HTTP
Hypertext Transfer Protocol

HTTP/S
Hypertext Transfer Protocol Secure

HTTPS
Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol
HTTP ist ein Protokoll für die Übermittlung von Informationen im Internet.

Hypertext Transfer Protocol over Secure Socket Layer
HTTPS ermöglicht eine sicherere HTTP-Kommunikation.

I

IANA
Internet Assigned Numbers Authority

ICMP
Internet Control Message Protocol

ID
Identität

IDE
Intelligent Drive Electronics

IDENT
IDENT ist ein Netzwerkprotokoll, mit dem ein Server feststellen kann, welcher Benutzer eines Mehrbenutzersystems eine bestimmte TCP-Verbindung geöffnet hat.

IDN
International Domain Name

IE
Internet Explorer

IKE
Internet Key Exchange

IM
Instant Messaging (Sofortnachrichten)

Internet Control Message Protocol
ICMP ist ein Teil der Internetprotokollfamilie und dient in Netz-

werken zum Austausch von Fehler- und Informationsmeldungen.

Internet Protocol
IP ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und bildet die erste vom Übertragungsmedium unabhängige Schicht der Internetprotokollfamilie.

Internet Relay Chat
IRC ist ein offenes Protokoll und ermöglicht eine direkte Kommunikation über das Internet.

Internetdienstanbieter
Ein ISP (Internetdienstanbieter) ist ein Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb im Internet erforderlich sind.

IP
Internet Protocol

IP-Adresse
Eine IP-Adresse (Internet-Protocol-Adresse) ist eine Nummer, die die Adressierung von Hosts und anderen Geräten in einem IP-Netzwerk erlaubt.

IPS
Intrusion Prevention System (Angriffschutzsystem)

IPsec
Internet Protocol Security

IRC
Internet Relay Chat

ISP
Internet Service Provider (Internetdienstanbieter)

L

L2TP
Layer 2 Tunneling Protocol

LAG
Link Aggregation Group (Linkbündelungsgruppe)

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

Link State Advertisement
LSA ist ein elementares Kommunikationsprinzip innerhalb des OSPF-Routing-Protokolls.

LSA
Link State Advertisement

LTE
3GPP Long Term Evolution

M

MAC
Media Access Control

MAC-Adresse
Eine MAC-Adresse (Media Access Control) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient.

Managed Security Service Provider
MSSPs bieten Sicherheitsdienste für Firmen an.

Management Information Base
Eine MIB ist eine Informationsstruktur zum Verwalten von Netzwerkgeräten (z.B. Router und Switches). Diese stellen Status-, Parameter-, Fähigkeits- und Steuerinformationen über sich selbst in einer MIB zusammen, die an anfragende Geräte gesendet wird.

Maskierung (Masquerading)
Maskierung ist eine Form von Network Address Translation, die es mehreren Computern (mit privaten IP-Adressen) in einem LAN ermöglicht, bei Verwendung einer einzigen öffentlichen IP-Adresse mit dem Internet zu kommunizieren.

MD5
Message-Digest-Algorithm 5

Message-Digest-Algorithm 5
MD5 ist eine kryptografische Hash-Funktion, die einen 128-Bit-Hashwert erzeugt.

MIB
Management Information Base

MIME
Multipurpose Internet Mail Extensions

MPLS
Multiprotocol Label Switching

MPPE
Microsoft Point-to-Point Encryption

MSCHAP
Microsoft Challenge Handshake Authentication Protocol

MSCHAPv2
Microsoft Challenge Handshake Authentication Protocol Version 2

MSP
Managed Service Provider

MSSP
Managed Security Service Provider

MTU
Maximum Tansmission Unit

Multipurpose Internet Mail Extensions
MIME ist ein Kodierstandard, der die Struktur und den Aufbau von E-Mails und anderer Internetnachrichten festlegt.

MX-Eintrag
Ein MX-Eintrag ist eine Art Ressourcen-Eintrag im Domain Name System (DNS), der festlegt, wie E-Mails über das Internet geroutet werden sollen.

N

NAS
Network Access Server

NAT
Network Address Translation

NAT-T
NAT-Traversal

Network Address Translation
System zur Wiederverwendung von IP-Adressen.

Network Time Protocol
NTP ist ein Protokoll für die Zeitsynchronisation von Computern in einem Netzwerk.

NIC
Network Interface Card (Netzwerkkarte)

Not-So-Stubby-Area
Eine NSSA ist ein Bereichstyp (area type) im Routingprotokoll OSPF.

NSSA
Not-So-Stubby-Area

NTLM
NT LAN Manager (Microsoft Windows)

NTP
Network Time Protocol

O

Open Shortest Path First
OSPF ist ein dynamisches Routing-Protokoll, das auf einem Link-State-Algorithmus basiert.

OpenPGP
OpenPGP ist ein Kryptografie-Protokoll basierend auf PGP (Pretty Good Privacy) zur Verschlüsselung von Informationen und Erzeugung digitaler Signaturen.

OSI
Open Source Initiative

OSPF
Open Shortest Path First

OTP
One-time password

OU
Organisational Unit

P

PAC
Proxy Auto Configuration (Automatische Proxy-Konfiguration)

PAP
Password Authentication Protocol

PCI
Peripheral Component Interconnect

PEM
Privacy Enhanced Mail

PGP
Pretty Good Privacy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PMTU
Path Maximum Transmission Unit

POP3
Post Office Protocol Version 3

Port
Ports sind Adresskomponenten, die in Netzwerkprotokollen eingesetzt

werden, um Datenpakete den richtigen Diensten (Protokollen) zuzuordnen. Genauer gesagt, dient ein Port als zusätzliche Identifikation – bei TCP und UDP ist es eine Zahl zwischen 0 und 65535 – die es einem Computer ermöglicht, zwischen mehreren verschiedenen gleichzeitigen Verbindungen zwischen zwei Computern zu unterscheiden.

Portscan
Der Vorgang, einen Netzwerkhost nach offenen Ports abzusuchen.

Post Office Protocol Version 3
POP3 ist ein Protokoll für die Übertragung von E-Mails in einem paketvermittelten Netzwerk.

PPP
Point-to-Point-Protokoll

PPPoA
PPP over ATM Protocol

PPTP
Point-to-Point Tunneling Protocol

Privacy Enhanced Mail
PEM ist ein frühes Protokoll zur Verschlüsselung von E-Mails mittels eines asymmetrischen Verschlüsselungsverfahrens.

Protokoll
Protokolle sind Regeln, die das Format, den Inhalt, die Bedeutung und die Reihenfolge gesendeter Nachrichten zwischen verschiedenen Instanzen (der gleichen Schicht) festlegen.

Proxy
Ein Proxy ist ein zwischengeschalteter Computer, der zur Pufferung, Überwachung und Zugriffskontrolle dient.

PSK
Preshared Key (verteilter Schlüssel)

Q

QoS
Quality of Service (Dienstqualität)

R

RADIUS
Remote Authentication Dial In User Service

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Remote Access Server

RBL
Realtime Blackhole List (Echtzeit-Blackhole-Liste)

RDN
Relative Distinguished Name

RDNS
Reverse Domain Name Service

RDP
Remote Desktop Protocol

Realtime-Blackhole-Liste (Echtzeit-Blackhole-Liste)
Eine RBL ist eine in Echtzeit abfragbare Schwarze Liste, die verwendet wird, um E-Mails zweifelhafter Herkunft als Spam zu klassifizieren. Die meisten Mailserver können so konfiguriert werden, dass die Nachrichten ablehnen oder markieren, die von einer Gegenstelle stammen, die auf einer oder mehreren schwarzen Listen geführt ist. Auch Webserver können Clients ablehnen, die auf einer schwarzen Liste stehen.

RED
Random Early Detection

Redundant Array of Independent Disks
Ein RAID-System dient zur Organisation mehrerer physikalischer Festplatten eines Computers zu einem logischen Laufwerk.

Remote Authentication Dial In User Service
RADIUS ist ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accounting von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient.

RFC
Request for Comment

Router
Ein Router ist ein Vermittlungsrechner, der in einem Netz dafür sorgt, dass bei ihm eintreffende Daten eines Protokolls zum vorgesehenen Zielnetz bzw. Subnetz weitergeleitet werden.

RPS
RED Provisioning Service

RSA
Rivest, Shamir & Adleman (Verschlüsselungstechnologie für öffentliche Schlüssel)

S

S/MIME
Secure/Multipurpose Internet Mail Extensions

SA
Security Associations (Sicherheitsverbindungen)

SAA
Sophos Authentication Agent

SCP
Secure Copy (aus dem SSH-Paket für Computeranwendungen für sichere Kommunikation)

SCSI
Small Computer System Interface

Secure Shell
SSH ist ein Protokoll bzw. Implementierung dieses Protokolls, mit dem sich eine verschlüsselte Netzwerkverbindung zu einem entfernten Computer aufbauen lässt.

Secure Sockets Layer
SSL und sein Nachfolger Transport Layer Security (TLS) sind Verschlüsselungsprotokolle für die sichere Datenübertragung im Internet.

Secure/Multipurpose Internet Mail Extensions
S/MIME ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail durch ein asymmetrisches Verschlüsselungsverfahren.

Security Parameter Index
SPI ist eine Identifikationsmarkierung, die zum Header (Kopfzeile) beim Tunneln von Daten mit IPsec hinzugefügt wird.

Sender Policy Framework
SPF ist eine Erweiterung des SMTP Protokolls SPF allows software to identify and reject forged addresses in the SMTP MAIL FROM (Return-Path), a typical annoyance of email spam.

Session Initiation Protocol
SIP ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das textorientierte Protokoll basiert auf HTTP und kann Signalisierungsdaten mittels TCP oder UDP über IP-Netzwerke übermitteln. Dadurch stellt es neben anderen Protokollen die Basis für Voice over IP, Videotelefonie und Multimedia-Anwendungen in Echtzeit bereit.

SFQ
Stochastic Fairness Queuing

SIM
Subscriber Identification Module

Simple Mail Transfer Protocol
SMTP ist ein Protokoll der Internetprotokollfamilie, das zum Austausch von E-Mails in Computernetzen dient.

Single Sign-On
SSO bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung auf alle Hosts und Dienste, für die er berechtigt ist, zugreifen kann, ohne sich jedes Mal neu anmelden zu müssen.

SIP
Session Initiation Protocol

SLAAC
Stateless Address Autoconfiguration

SMB
Server Message Block

SMP
Symmetrisches Multiprocessing

SMTP
Simple Mail Transfer Protocol

SNAT
Source Network Address Translation

SNMP
Simple Network Message Protocol

SOCKetS
„SOCKS“ ist eine Abkürzung für „SOCKetS“, ein Protokoll, das es Client-Server-Anwendungen erlaubt, transparent die Dienste einer Firewall zu nutzen. SOCKS, oft auch Firewall Traversal Protocol genannt, befindet sich momentan in Version 5 und muss clientseitig vorhanden sein, um richtig zu funktionieren.

SOCKS
SOCKetS

Sophos UTM Manager
Software für die Überwachung und Verwaltung von mehreren UTM-Geräten über eine einzige Software-Oberfläche. Früher bekannt unter Astaro Command Center.

Source Network Address Translation
SNAT ist ein Spezialfall von Network Address Translation (NAT), bei dem die Quell-IP-Adresse ersetzt wird.

Spanning Tree Protocol
Netzwerkprotokoll, das Bridge-Loops erkennt und verhindert

SPF
Sender Policy Framework

SPI
Security Parameter Index

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

STP
Spanning Tree Protocol

SUA
Sophos User Authentication

Subnetzmaske
Die Subnetzmaske (auch Netzwerkmaske oder Netzmaske genannt) eines Netzwerks legt fest, welche Adressen Teil des lokalen Netzwerks sind und welche nicht. Einzelne Computer werden auf Basis dieser Definition einem Netzwerk zugeordnet.

SUM
Sophos UTM Manager

Symmetrisches Multiprocessing
Der Einsatz von mehr als einem Prozessor.

SYN
Synchronous

T

TACACS
Terminal Access Controller Access Control System

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

Time-to-live (TTL)
TTL ist der Name eines 8-Bit-langen Header-Felds des Internetprotokolls (IP) und gibt an, wie lange ein Paket auf dem Weg vom Ziel zum Sender unterwegs sein darf, bevor es verworfen wird, und soll verhindern, dass unzustellbare Pakete unendlich lange weitergeroutet werden.

TKIP
Temporal Key Integrity Protocol

TLS
Transport Layer Security

TOS
Type of Service

Transmission Control Protocol
TCP ist ein Protokoll der Internet-Protokollfamilie, das zusammen mit dem Internetprotokoll (IP) eingesetzt wird, um Daten in Form von Paketen zwischen Computern über das Internet zu transportieren. Das Protokoll gewährleistet eine verlässliche und geordnete Auslieferung von Daten vom Absender zum Empfänger.

Transport Layer Security
TLS und sein Vorgänger Secure Sockets Layer (SSL) sind Verschlüsselungsprotokolle für die sichere Datenübertragung im Internet.

TTL
Time-to-live (TTL)

U

UDP
User Datagram Protocol

UMTS
Universal Mobile Telecommunications System

Unified Threat Management
Software für Unified Threat Management, die Mail- und Internetsicherheit umfasst. Früher bekannt unter Astaro Security Gateway.

Uniform Resource Locator
URLs identifizieren eine Ressource in Computernetzwerken und sind der Standard von Adressen im Internet.

Unterbrechungsfreie Stromversorgung
Ein Gerät zur unterbrechungsfreien Stromversorgung (USV) wird eingesetzt, um bei Störungen der Stromversorgung einen durchgehenden Betrieb zu ermöglichen.

Up2Date
Ein Dienst, der es erlaubt, relevante Aktualisierungspakete vom Sophos-Server herunterzuladen.

URL
Uniform Resource Locator

USB
Universal Serial Bus

User Datagram Protocol
UDP ist ein Protokoll für den verbindungslosen Datenaustausch, das hauptsächlich für die Verteilung von Nachrichten über ein Netzwerk verwendet wird.

USV
Unterbrechungsfreie Stromversorgung

UTC
Coordinated Universal Time (Koordinierte Weltzeit)

UTM
Unified Threat Management



V

VDSL
Very High Speed Digital Subscriber Line

Vereinbarter Schlüssel
Ein vereinbarter Schlüssel (shared secret) ist ein Kennwort, das von zwei Gegenstellen zur sicheren Kommunikation geteilt wird.

Virtuelles Privates Netzwerk
Ein VPN (Virtual Private Network) ist eine verschlüsselte Verbindung zwischen zwei Standorten, die zum Transport privater Daten ein öffentliches Netz wie das Internet nutzt.

VLAN
Virtuelles LAN

VNC
Virtual Network Computing

Voice over IP
Mit VoIP wird sprachbasierte Kommunikation (Telefonieren) über Computernetzwerke geroutet.

VoIP
Voice over IP

VPC
Virtual Private Cloud

VPN
Virtuelles Privates Netzwerk



W

WAF
Web Application Firewall

WAN
Wide Area Network

W-CDMA
Wideband Code Division Multiple Access

WebAdmin
Webbasierte grafische Benutzeroberfläche von Sophos/Astaro-Produkten wie UTM, SUM, ACC, ASG, AWG und AMG.

WEP
Wired Equivalent Privacy

Windows Internet Naming Service
WINS ist ein von Microsoft entwickeltes System zur dynamischen Auflösung von NetBIOS-Namen.

WINS
Windows Internet Naming Service

WLAN
Wireless Local Area Network (Drahtloses lokales Netzwerk)

WPA
Wi-Fi Protected Access



X

X.509
X.509 ist ein Standard für digitale Zertifikate, der von der ITU-T (International Telecommunications Union –

Telecommunication) herausgegeben wird. Dort sind Informationen und Attribute spezifiziert, die zur Identifikation einer Person oder eines Computers erforderlich sind.

XSS
Cross-Site-Scripting

Abbildungsverzeichnis

Bild 1 WebAdmin: Initiale Anmeldeseite 24
Bild 2 WebAdmin: Reguläre Anmeldeseite 25
Bild 3 WebAdmin: Dashboard 28
Bild 4 WebAdmin: Übersicht 31
Bild 5 WebAdmin: Beispiel einer Liste 34
Bild 6 WebAdmin: Beispiel eines Dialogfelds 37
Bild 7 WebAdmin: Ziehen eines Objekts aus der Objektliste Networks 40
Bild 8 MyUTM-Portal 65
Bild 9 Lizenzen: Abonnement-Warnhinweis 70
Bild 10 Up2Date: Fortschrittsfenster 74
Bild 11 Benutzerportal: Begrüßungsseite 82
Bild 12 Anpassung: Beispiel einer blockierten Webseite mit Angabe der anpassbaren Elemente 90
Bild 13 Anpassung: HTTP-Download-Seite Schritt 1 von 3 Datei wird heruntergeladen 94
Bild 14 Anpassung: HTTP-Download-Seite Schritt 2 von 3 Virenscan 94
Bild 15 Anpassung: HTTP-Download-Seite Schritt 3 von 3 Herunterladen der Datei abgeschlossen 95
Bild 16 Anpassungen: Blockierte POP3-Proxy-Nachricht 97
Bild 17 Gruppen: eDirectory-Browser von Sophos UTM 132
Bild 18 Authentifizierung: Microsoft Management-Konsole 140
Bild 19 Email Encryption: Mit zwei Sophos UTM-Geräten 390
Bild 20 Mail-Manager von Sophos UTM 410
Bild 21 Endpoint Protection: Übersicht 420
Bild 22 Mesh-Netzwerk, eingesetzt als WLAN-Bridge 454
Bild 23 Mesh-Netzwerk, eingesetzt als WLAN-Repeater 454
Bild 24 RED: Aufbaukonzept 493
Bild 25 LAN Modus: Ohne Tags 501
Bild 26 LAN Modus: Ohne Tags, mit Tags verwerfen 501
Bild 27 LAN Modus: mit Tags 501
Bild 28 LAN Modus: nicht verwendet 502
Bild 29 RED 50: Hostnamen- und Uplink-Lastverteilung (türkis) und Hostnamen- und Uplink-Failover (rot) 505
Bild 30 RED 50: Hostnamen-Lastverteilung und Uplink-Failover (grün) sowie Hostnamen-Failover und Uplink-Lastverteilung (blau) 505

Bild 31 Berichte: Beispiel eines Liniendiagramms 580
Bild 32 Berichte: Beispiel eines Tortendiagramms 580

Stichwortverzeichnis

3

3DES, Verschlüsselung 517, 559
3G/UMTS (interface type)
  failover uplink 503
3G/UMTS (Schnittstelle) 159, 162
  MTU 163

A

Ablaufzeit, Bridging 191
Abmelden 627
  automatische 627
Abonnements, Lizenz 64
  aktivieren 66
  BasicGuard 69, 71
  Email Protection 71
  Informationen zu 71
  Network Protection 71
  Web Protection 71
  Webserver Protection 71
  Wireless Protection 71
Absender-Blacklist, Bereich im Benutzerportal 634
Absender-Whitelist, Bereich im Benutzerportal 633
Abteilungen, Berichte 598
Access Points 439, 446-447
  active 447
  Arten 446
  ausstehende 441
  authentifizieren an 440-441
  authorization of 447
  Berichte 604
  channel 449
  Clients *Siehe:* WLAN-Netzwerke, Clients
  country setting 448
  deletion of 447
  disabling of 447
  ETSI 446
  FCC 446
  grouping of 448
  gruppieren 452
  inactive 447
  konfigurieren 439
  label of 448
  Land einstellen 447
  Mesh-Access-Points 453
  network assignment 451
  Netzwerkschnittstelle 440
  pending 447-448
  Root-Access-Points 453
  SSID 442
  Status 439
  Verschlüsselung 442
    Algorithmen 444
    Kennwort 442
    WEP 442-443
    WPA/WPA2 442
Active Directory 134, 138
  Backend-Server 138
  BaseDN 140
  Domänenbeitritt 147
  Email-Empfänger-Verifizierung 352, 372
  FTP-Proxy und 345, 347
  Gruppen 154
  Portnummer 138
  prefetching with 154
  Single Sign-On 135, 146
  unterstützte Versionen 138
Active Directory Group Membership Syncronization 155
Admin-Kennworteinrichtung (Dialogfenster) 56
Administrationshandbuch *Siehe:* Administratorhandbuch
administrator
  contact data 93

password of
setting of 24
Administrator 126
Kennwort 55
Kontaktdaten 91
WebAdmin-Zugriff 57
Administratorhandbuch
herunterladen 621
Sprache auswählen 622
ADSL 173
advanced threat protection 42, 272
Berichte 589
Advanced Threat Protection 272
activation of 272
Live-Protokoll 273
AES, Verschlüsselung 517, 559
Agent, SNMP 99
AH (Protokoll) 516, 558
Aktivierungsschlüssel, Lizenz 65
Aliasse, IP-Adressen 178
Amazon VPC 512
aktivieren 512
setup of 513
Status 512
Verbindungen 512
import of 513

Ä

Änderungen, der WebAdmin-Einstellungen 49
Anfragerouten 239
Angriffe, Intrusion Prevention 41-42
Angriffe 274-275
Signaturen 274
Angriffschutzsystem *Siehe:* IPS
Angriffsversuche 41
Anmeldeprobleme 627
Anmeldeseite
Standard- 29
Anonymisierung, Berichtsdaten 601, 603-604, 618
Anpassungen
der POP3-Nachrichten 90
der Quarantäne-Statusmeldungen 90
der Systemmeldungen 89
der Webfilter-Meldungen 90
des Quarantäneberichts 90
des Unternehmenslogos 90
des Unternehmenstexts 91
Home-Use-Lizenz und 89
home use license and 407
Antispam-Mechanismus 356, 378
Ausdruckfilter 358, 379
BATV 360, 369
Blacklisting 128, 358, 379, 634
fehlende RDNS-Einträge ablehnen 359
Greylisting 359
RBLs 357
Spam-Kennzeichnung 358, 379
Spamfilter 357, 378
SPF-Prüfung 360
Status 43
ungültige HELO ablehnen 359
Whitelist 128, 405, 408, 633
antispam engine
Ausdruckfilter 374
BATV 372
blacklisting 83, 373
extra RBLs 372
greylisting 372
RBLs 372
rejection of invalid HELO 372
rejection of missing RDNS entries 372
Spamfilter 373
SPF check 372
whitelisting 83
Antispyware-Mechanismus
Spyware blockieren 42
Status 43
antispyware engine
settings of 27
Antiviren-Mechanismus
des FTP-Proxys 344-345

des POP3-Proxys 377
des SMTP-Proxys 352
des Webfilters 311
deaktivieren 324
maximale E-Mail-Größe 377
scannen
von E-Mails 353, 377
Status 43
von Endpoint Protection 427
Zip-Archive, verschlüsselt 310, 345
antivirus engine
encrypted files 334
of web application firewall 479
scanning 55
of downloads 479
of emails 373
of uploads 479
settings of 27, 55
unscannable files 334
AonSpeed (ISP) 174
APC (Hersteller) 17
AppAccuracy, application control 64
Apple OpenDirectory SSO (Web Filter authentication mode) 337
appliances
default settings 23
Appliances
Modelle 106
Application Control 339
AppAccuracy 64
Ausnahmen 343
Berichte 600
Netzwerksichtbarkeit 42, 340
Regeln 47, 197, 340, 342-343
Application Control (Web Filter message) 92
Arbeitsplatzrechner 15
Arbeitsplatzrechner, für Verwaltung 15
Arbeitsspeicher
Speicherplatzbelegung 583
Systemanforderungen 16
ARP
ARP-Bekanntgabe (gratuitous) 106
Auflösung, falsche 158
Broadcasts und Bridging 190
Cache 106
Clashes 158
Hochverfügbarkeit und 106
Assistent 28
audio content, filtering 374
Audioinhalte, filtern 354
Auditor (Benutzerrechte) 59
Auditor (Benutzerrolle) 58
Ausdruckfilter, POP3-Proxy 379
Ausdruckfilter, SMTP-Proxy 358
Ausfallsicherung, Hochverfügbarkeit 104, 106
ausführbare Dateien filtern 354
ausgelagertes Protokollarchiv 612
E-Mail 613
FTP-Server 612
SMB-Freigabe 612
SSH-Server 613
Ausnahmen
Application Control 343
bei Berichten 617
FTP-Proxy 345, 347
POP3-Proxy 380-381
Quarantänebericht 407
SMTP-Proxy 363
Webfilter 323, 325-326, 333
Standardmodus und 324
Transparenzmodus und 324
ausstehende Access Points 441
Ausstehende Access Points 447-448
authentication servers
Active Directory 134
eDirectory 134
LDAP 134
RADIUS 134
TACACS+ 134
Authentifizierung 134-135
Agent für 132
allgemeine Einstellungen 134

Cache für 135
löschen 135
IPsec 520, 522
Live-Protokoll 136
SOCKS-Proxy 292
timeout 334
von Benutzern 127
von Clients 115, 117, 132
Web Application Firewall 487, 491
Webfilter 324, 334
Apple OpenDirectory SSO 337
Authentifizierungsalgorithmen
Internet Key Exchange 524, 563
IPsec 525, 565
WPA/WPA2-Enterprise 440-441
Authentifizierungsdienste 115, 144
external 134
Authentifizierungsserver 136
Active Directory 138
eDirectory 136
externe 115
LDAP 141
RADIUS 134, 143, 441
TACACS+ 145
automatische Aushandlung, Schnittstellen 187
automatische Backups 81
Erstellungsintervall 81
herunterladen 82
Kennwortschutz 82
löschen 81-82
speichern 81
verschlüsseln 81
versenden 81
wiederherstellen 82
autorisieren
von Benutzern 144-145
AV-Mechanismus *Siehe:* Antiviren-Mechanismus

B

Backend-Server
Active Directory 138
eDirectory 136
LDAP 141
RADIUS 143
TACACS+ 145
Backend-Verzeichnisdienste *Siehe:* Verzeichnisdienste
Backup-Uplink 180
backups
restoration of 25
Backups
als Vorlagen 80
automatische 81
Erstellungsintervall 81
herunterladen 82
Kennwortschutz 82
löschen 81-82
speichern 81
verschlüsseln 81
versenden 73, 81
vor Up2Date-Installation 73
wiederherstellen 82
Dateierweiterungen 78
erstellen 77, 79
Ersteller 78, 82
herunterladen 78
importieren 79-80, 82
Inhalt 77-78
Kennwortschutz 78
Lesbarkeit 77
löschen 79
speichern 77
Sperrdateien und 79
SSH-DSA-Schlüssel und 613
verfügbare 78, 81-82
verschlüsseln 78
versenden 79
Empfänger 79
Versionsnummer 78

vertrauliche Informationen und 78
wiederherstellen 28, 77-78
von USB-Flashspeicher 78
Bandbreiten-Pools, Dienstqualität 47, 198
Bandbreitenmonitor *Siehe:* Flow-Monitor
Bandbreitennutzung, Berichte 585
basic system setup 24
BasicGuard, Abonnement 69, 71
Basislizenz 71
Batteriebetrieb, USV 17
BATV 360, 369, 372
Bedrohungsstatus 41
Benachrichtigungen 50, 87-88
Arten 88
beschränken 87
Codes 87
Empfänger 87
gerätespezifischer Text 88
Lizenz und 72
logging and 610
per E-Mail 87-88
Smarthosts und 88
SNMP-Trap 87-88
Benutzer 115, 125-126
aktuell eingeloggt 33
Authentifizierung 127
automatisch anlegen 135
autorisieren 144-145
Benutzergruppen 115, 125, 129
deaktivieren 127
Kennwort
ändern 642
einstellen 127
password
change of 84
Zertifikat 128
Benutzerdefinitionen 126
Administratorrechte 128
Backend-Synchronisierung 127
E-Mail-Adressen und 126
Infosymbol 126
Benutzereinstellungen 61
Benutzeroberfläche 20
Benutzerportal 82, 629
Begrüßungstext 86
blacklisting of email addresses 83
Client-Authentifizierung 84, 638
configuring one-time password 629, 638
Cookies 86
E-Mail-Adressen auf Blacklist 128, 634
E-Mail-Adressen auf Whitelist 128, 633
E-Mail-Protokoll 632
E-Mail-Quarantäne 630
E-Mails freigeben
Nutzerbeschränkung 632
email log 83
email quarantine 83
Fernzugriff 84, 569, 639
Konfigurationsdateien 543-544
software 84
Hostname 85
Hotspots 83, 635
HTML5-VPN-Portal 84, 640
IPsec client installation instructions 561
Kennwort ändern 642
L2TP-Client-Installationsanleitung 555
Lausch-Adresse 86
logout of 84
Mail-Quarantäne 630
Menü 86
one-time passwords 84
OTP-Token 84
POP3-Konten 83, 633
Portnummer 85
PPTP-Client-Installationsanleitung 549
SMTP-Protokoll 83, 632
Sprache auswählen 85
SSL-Client-Installationsanleitung 545
Web Application Firewall und 86
Web Filter CA certificate 84
Webfilter-CA-Zertifikat 642
whitelisting of email addresses 83
Zertifikat 60
Zugriffskontrolle 85, 135

Benutzerrechte 59
  Auditor 59
  Manager 59
Benutzerrollen 58
  Auditor 58
  Readonly 58
Berichte 579
  Access Points 604
  advanced threat protection 589
  aktivieren 614
  Ausnahmen 617
  Bandbreitennutzung 585
  deaktivieren 614
  Diagramme 580
  E-Mail-Nutzung 602
  E-Mail-Verkehr 601
  E-Mails, blockierte 603
  Email Protection 601-604
  Fernzugriff 605-606, 616
  Firewall 587-588
  Gesamtberichte 608
  Hardware-Informationen 105, 582-584
  Intrusion Prevention 587, 589
  IPFIX 616
  konfigurieren 50, 614
  Liniendiagramme 580
  Network Protection 586-587
  Netzwerknutzung 105, 584-585
  Netzwerkverkehr 584-585
  Netzwerkverkehrsdaten 105
  Quarantänebericht 405-409
  Tortendiagramme 580
  Web Application Firewall 607
  Web Protection 590, 601
    Abteilungen 598
    Application Control 600
    Datensammlung 295
    geplante Berichte 599
    Internetnutzung 590
    Suchmaschinen 595
  Webserver Protection 607
  Wireless Protection 604-605
  Zeiteinstellungen 50
  Zeitlücken 51
  Zeiträume 614
Berichtsdaten
  anonymisieren 601, 603-604, 618
  automatisch löschen 614
  entanonymisieren 601, 603-604, 618
  Fernzugriff 616
  herunterladen 586, 588-590, 592, 596, 601-603, 606, 608, 616
  Hochverfügbarkeit und 105
  sending of 592, 596
  zurücksetzen 56
Betriebsstatus, System 41
BGP *Siehe:* Border Gateway Protocol
Bitmaske 119
Blacklist (Web Filter message) 91
Blacklisten von E-Mail-Adressen 128, 358, 379, 634
blacklisting, email addresses 83, 373
blocked file 374
blocked IP address, due to failed logins 153
Blowfish (Verschlüsselung) 78
Border Gateway Protocol 223
  aktivieren 224
  autonome Systeme, mehrere 224, 230
  Fehlersuche-Informationen 231
  Filterlisten 229
  IP-Adressen-Übereinstimmung, strikte 230
  Multi-Pfad-Routing 231
  Neighbor-Router 225
  Peer-Router 225
  Routemaps 227
Bridging 22, 188
  Ablaufzeit 191
  ARP-Broadcasts 190
  configuration of 189
  EtherTypes, weiterleiten von 191
  Firewallregeln 189
  IPv6 und 191
  removal of bridge 190

removal of interfaces 190
Spanning Tree Protocol 191
status of 189
virtuelle MAC-Adresse 189, 191
with RED appliances 508
WLAN 453
Broadcasts, Firewall und 259
Browser *Siehe:* Webbrowser
Bypass Content Block (Web Filter message) 93
bypassing blocked content, HTTP proxy authentication timeout 334

C

CA (Zertifizierungsinstanz) 536, 539
herunterladen 540
importieren 540
Signierungs-CA 539
für VPN 541
Verifizierungs-CA 539
WebAdmin-Zertifikat 59
Webfilter-Zertifikat 642
cache
of Web Filter 336
Cache
des Webfilters 324
für Authentifizierung 135
löschen 135
für Up2Dates 76
CBC-Modus (Cipher Block Chaining) 78
CD-ROM-Laufwerk, Systemanforderungen 16, 19
CD-ROM, für Installation 17
Certificate Authority (Zertifizierungsstelle) 24, 329
fingerprint 333, 395
Signierungs-CA 330
verification CA 332
Web Filter certificate 84
WebAdmin certificate 24
Cisco VPN Client 574
Fehlersuche-Informationen 576-577
iOS-Konfiguration 575-577
Konfiguration 574-575
Live-Protokoll 575
Client-Authentifizierung 84, 115, 117, 132
Client-Authentifizierung, Bereich im Benutzerportal 638
Cluster, Hochverfügbarkeit 104, 106
hotspots and 457
Knoten 104, 107
Ressourcennutzung 108
Systemstatus 108
Status 43
clusters, high availability 109
autojoin 109
configuration of 108
of master 110, 112
deactivation of 111
nodes 109
Codes, von Benachrichtigungen 87
Community String, SNMP 99, 101
company information 24
complexity, password 153
confidentiality footer, SMTP proxy 374
connection types, for Internet uplink 26
contact data, administrator 93
Controller
IDE 19
SCSI 19
Cookie-Signierung 478
Outlook Web Access 482
Schlüssel 486
secret of 478
Country-Blocking 260
Ausnahmen 261
CPU-Auslastung 41, 108, 583
CPU, Systemanforderungen 16, 19
CRL *Siehe:* Zertifikate, Sperrlisten (CRLs)
Cross-Site-Scripting
Schutz vor 471
cross-site scripting
protection from 481
CSV-Export, Trennzeichen 616

D

Dashboard 28, 32, 41
Aktualisierungsintervall 43
Gruppieren von Informationen 45
konfigurieren 43
RAID-Anzeige 17
Sophos Newsfeed 44
data protection configuration 375
Dateierweiterungen
blockieren 310, 344-346
deaktivieren 324
filtern 355, 378
von Backups 78
Datenbanken, Zurücksetzen von 56
Datenpakete *Siehe:* Pakete
Datenübertragungsrate, Netzwerkkarten 42
Datenverkehrsmonitor *Siehe:* Flow-Monitor
Datum 50
einstellen 20
manuell 50, 52
NTP-Server 50, 52
Dead Peer Detection, IPsec 529, 567
default gateway, for external interface 26
default settings, appliances 23
Definitionen 115
von Diensten 115, 122
von MAC-Adressen 121
von Netzwerken 115-116
von Zeiträumen 115, 124
Denial of Service *Siehe:* DoS, Intrusion Prevention
DER (Dateiformat) 396
Destination Address
Translation *Siehe:* DNAT
Device Control, Endpoint Protection 431
DHCP 243
Anfragen weiterleiten 247
HTTP-Proxy, automatische Browser-Konfiguration 246
IP-Adressenpool 117
Lease-Tabelle 248, 250
IPv4 248
IPv6 250
Leases und Präfix-Bekanntmachungen 250
mit WLAN-Netzwerken 440, 456
Optionen 251
Relays 247
Server 26, 244
statische Zuordnungen 248-251
Web Filter browser configuration, automatic 335
with RED appliances 506-507
Diagramme, Berichte 580
Dialogfenster, WebAdmin 37
Dienstdefinitionen
erstellen 122
Infosymbol 122
namens „Web Surfing“ 440
Typ ändern 124
Dienste
definieren 115, 122
mit AH 124
mit ESP 123
mit ICMP 123
mit IP 123
mit TCP 122
mit UDP 122
Netzwerkdienste 237
Dienstgruppen 122, 124
Dienstqualität (QoS) 191, 201
aktivieren 192
Bandbreiten-Pools 198
Download-Drosselung 200
ECN 202
Schnittstellen 192
Status 192
Verkehrskennzeichner 193
dig (network tool) 624
Directory-Traversal, Schutz vor 471
directory services 134
Active Directory 134

eDirectory 134
LDAP 134
RADIUS 134
TACACS+ 134
Distinguished Name 137, 139, 141, 536
DKIM, SMTP-Proxy 368
DN *Siehe:* Distinguished Name
DNAT 268, 290
Firewall und 259
Firewallregeln und 269
PPTP-Zugriff und 268
DNS 237
Cache, löschen 238
DNSSEC 237
DynDNS 240
Einträge, Lebensdauer 238
Gruppen 119
Hostname des Systems und 50
hosts 624
Hosts 118
Time-to-live (TTL) 118
lookup 624
Web Filter and 334
Lookups 623
Proxy 292
Reverse-DNS 118
Server 238
Fernzugriff 577
interne 237, 239
Root- 238
zugelassene Netzwerke 237
statische Zuordnungen 240
Weiterleitungen 238-239
vom Internetanbieter 238
WLAN-Netzwerke 440
Zoneninformationen 238
Dokumentation, Administrator 621
domains, SMTP 27
Domänencontroller *Siehe:* Verzeichnisdienste
DoS, intrusion prevention 153
DoS, Intrusion Prevention 276
Download-Drosselung, Dienstqualität (QoS) 48, 200
Download-Verwaltung, Webfilter 93
Download Complete (Web Filter message) 92
Download in Progress (Web Filter message) 92
download manager, Web Filter 334
download size 92
downloads, antivirus scanning 479
DSA-Schlüssel, SSH 613
Backups und 613
öffentliche 613
DSL
ADSL 173
VDSL 170
DSL (PPPoA/PPTP) (Schnittstelle) 160, 173
MTU 174
DSL (PPPoE) (Schnittstelle) 160, 170
MTU 171
Multilink 172
dynamische Adresszuweisung 159
dynamische IP-Endpunkte 118
dynamisches Routing (OSPF) *Siehe:* OSPF
DynDNS 240

E

E-Mail-Adressen
Blacklist 128, 358, 379, 634
einzigartige 135
Konflikte 135
Whitelist 128, 405, 633
E-Mail-Domänen 350
E-Mail-Empfänger
verifizieren 352, 361
von Backups 73
von Gesamtberichten 609
von Hotspot-Kennwörtern 461, 635
von Protokolldatei-Archiven 613
von Web-Protection-Berichten 599
E-Mail-Entschlüsselung 388

E-Mail-Fußzeilen
- Antivirenprüfung 355
- Format 369

E-Mail-Protokoll
- im Benutzerportal 632

E-Mail-Quarantäne 353, 377
- Berichte 603
- E-Mails freigeben 353, 377, 405-406, 630
- Fehlfunde 405
- im Benutzerportal 630
- POP3-Quarantänebericht 407
- Verteilerlisten 407

E-Mail-Relays 365-366
- Antiviren-Scan 366
- Authentifizierung 365
- Blacklist 366
- hostbasierte 365
- Upstream-Hosts 365

echte Webserver 471, 475-476
- manuell hinzufügen 475

Echte Webserver
- matching virtual webservers 473

Echtzeit-Blackhole-Listen *Siehe:* RBLs

ECN (Explicit Congestion Notification)
- Dienstqualität (QoS) 202
- IPsec 522

eDirectory 134, 136
- Backend-Server 136
- BaseDN 137
- Gruppen 154
- Portnummer 137
- prefetching with 154
- Single Sign-On 147

eingebettete Objekte, in Webseiten
- entfernen 324

Einstellungen
- Benutzer- 61

email address, of cache administrator, web messages 93

email addresses
- blacklisting of 83, 373
- whitelisting of 83

Email Encryption 355, 368, 386, 389
- aktivieren 390
- CA erstellen 390
- entschlüsseln 388
- interne Benutzer 392
- konfigurieren 389
- OpenPGP 391, 396
  - öffentliche Schlüssel 396
  - Schlüsselserver 391
- S/MIME
  - authorities 394
  - public keys 394-395
  - Zertifikate 391, 395
- Standardrichtlinien festlegen 391
- Zertifikate 395
  - automatisch extrahieren, S/MIME 391
  - Informationen, enthaltene 50
- zurücksetzen 390

email encryption, SPX 398
- Benachrichtigungen 401
- Konfiguration 399
- notification subject 403
- password 400
- password expiry 400
- password settings 402
- password, SPX
  - password reset 400
- portal settings 400
- reply portal 400, 404
- reply portal settings 404
- send notification 401
- templates 375, 401
- unused password 400

email messages, customization of 97

Email Protection 349
- Abonnement 71
- Berichte 601-604
- data protection 361
- Mail-Manager 410
- POP3-Proxy 375
- Quarantänebericht 405
- settings of 27

SMTP-Proxy 349
SPX encryption 398
Benachrichtigungen 401
Konfiguration 399
notification subject 403
password 400
password expiry 400
password reset 400
password settings 402
portal settings 400
reply portal 400, 404
templates 401
statistics 349
Verschlüsselung 386
email quarantine 82
high availability and 109
Mail-Manager 411
release of emails 83
email recipients
of RED unlock code 495
verification of 371
Email Released From Quarantine (SMTP proxy message) 97
Empfänger
von Benachrichtigungen 87
von E-Mails *Siehe:* E-Mail-Empfänger
Empfängerverifizierung, SMTP-Proxy 352, 361
Endbenutzerportal *Siehe:* Benutzerportal
Endpoint Protection 419, 421
activation of 421
aktivieren 435-436
Antiviren-Mechanismus 427
Antivirenrichtlinien 427
antivirus exceptions 429
Computerverwaltung 421, 423-424
Agent installieren 423
Computer gruppieren 424
default group 426
deactivation of 421
deaktivieren 435-436
Device Control 431
Ausnahmen 432
Richtlinien 431
installation on endpoints 423
Live-Protokoll 420
registration at Sophos LiveConnect 426
Status 43
tamper protection 426
Übergeordneter Proxy 427
UTM ID, resetting of 56
Web Control 435-436
Entanonymisierung, Berichtsdaten 601, 603-604
Enterprise Toolkit, installieren 21
Entschlüsselung, E-Mail 388
Erkennung, Hardware 18-19
Error While Releasing Email From Quarantine (SMTP/POP3 proxy message) 97
ESP (Protokoll) 516, 558
Ethernet-DHCP (Schnittstelle) 160, 168
MTU 169
Ethernet-Statisch (Schnittstelle) 160, 164
MTU 165
Proxy-ARP 165
Ethernet-VLAN (Schnittstelle) 160, 166
MTU 167
Proxy-ARP 167
Ethernet, Betriebsmodi 187
EtherTypes 191
Excel (Format)
Berichtsdaten herunterladen in 586, 588-590, 592, 596, 601-603, 606, 608
Trennzeichen 616
executables, filtering 374
expression filter, SMTP proxy 374
external interfaces 26
externe Netzwerke 157
externe Schnittstellen 157

F

Failover, Linkbündelung 179
Fehlfunde, Quarantäne-E-Mails 405

Fernzugriff 543
Berichte 605-606
Berichtsdaten von 616
certificates for 24
Cisco VPN Client 574
clientloses SSL-VPN 569
DNS-Server 577
Domänenname 577
HTML5-VPN-Portal 569-570
IPsec 557
Konfigurationsdateien für Benutzer 543, 639
L2TP über IPsec 552, 556
PPTP 548-551
section in User Portal 84
SSL-VPN 544, 546
statische IP-Adresse für Benutzer 128
Status 43, 543
WINS-Server 577
Zertifikate für 126
Fernzugriff, Bereich im Benutzerportal 639
Festplatte
Größe und Typ 19
löschen 21
Speicherplatzbelegung 41, 108
Systemanforderungen 16
File Extension (Web Filter message) 92
file extensions
filtering of 374
File Size (Web Filter message) 92
Filterfeld, in Listen 35
Filtering Options, Web Filter 323
fingerprint, certificate authorities 333, 395
Firewall 42, 255
Berichte 587-588
Broadcasts und 259
Country-Blocking 260
Ausnahmen 261
Fehlersuche-Informationen 258
Helfer für Verbindungsverfolgung 264
ICMP 262
IDENT-Verkehr und 259
Internetzugriff 268
konfigurieren 259
Live-Protokoll 258
NAT und 259
Protokollhandhabung 265
Protokollierungsoptionen 266
Sicherheitsrichtlinie 255
firewall profiles, web application firewall 476, 482
Firewallregeln 255-256
„Any“-Regeln 256
aktive 42
ändern 258
automatische 256
DNAT und 269
erstellen 256
Fehlersuche-Informationen 258
für Bridging 189
löschen 258
Regelabgleich 256
sortieren 256
Firmware-Aktualisierungen 72, 74
herunterladen 74-75
installieren 73-75
planen 74
Firmware-Version 41, 74
Flood-Schutz, Angriffschutz 276
ICMP 278
SYN 277
UDP 278
Flow-Monitor 42, 45
anpassen 163, 165, 168, 170, 172, 175, 177
Form-Hardening 479, 482
Form Hardening
Schlüssel 486
Forwarders, DNS 238
FQDN 577
Hostname und 50
FTP 344
Clients 291
Helfer für Verbindungsverfolgung 265

Server 347
als Protokollarchiv 612
von Sophos UTM 76
FTP-Proxy 344
Active Directory und 345, 347
aktivieren 344
Antiviren-Mechanismus 344-345
Ausnahmen 345-347
Betriebsmodi 344
Blockieren von Dateierweiterungen 344, 346
maximum scanning size 345
Server 347
full transparent (Web Filter operation mode) 303

G

generischer Proxy 290
GeoIP 260
geplante Berichte 599
Geräteinformationen, SNMP 99
Gesamtberichte 608
ansehen 608
Anzahl 615
archivierte 608
generieren 608
konfigurieren 608, 615
PDF-Einstellungen 616
Geschwindigkeit von Verbindungen, steigern 179
Gewichtung
Server-Lastverteilung 286
Uplink-Ausgleich 181
gratuitous ARP 106
greylisting 372
Greylisting 359
Grundkonfiguration 15, 22
Backup-Wiederherstellung 28
Gruppen
Benutzergruppen 129
Dienstgruppen 122, 124
DNS-Gruppen 119
Multicast-Gruppen 119
Netzwerkgruppen 119
Verfügbarkeitsgruppen 119
Guest (WLAN-Netzwerk) 440

H

H.323 289
Helfer für Verbindungsverfolgung 289
HA *Siehe:* Hochverfügbarkeit
Handbuch, Administrator- 621
Sprache auswählen 622
Hardware
Berichte 105, 582-584
Mindestanforderungen 15, 19
Schnittstellen 187
Störung, Umgang mit 104
Hardware-Appliances, Slotinformation 161
Hardware-Erkennung 18-19
Hardwarekompatibilitätsliste 16-17, 106, 166, 621
Hardwareschnittstellen 161
HCL *Siehe:* Hardwarekompatibilitätsliste
HDD *Siehe:* Festplatte
Heartbeat-Anfragen, Hochverfügbarkeit 105
Helfer für Verbindungsverfolgung 264
H.323 289
SIP 287
HELO, invalid 372
HELO, ungültiges 359
Herunterfahren, System 55, 112
nach Werkszurücksetzung 56
High Availabilty (Hochverfügbarkeit)
active-active 109
active-passive 109
autojoin 109
backup interfaces 112
clusters 109
configuration of 108
automatic 108-109, 111
of master 110, 112
up2date rollback 111
deactivation of 111

hot standby 109
master-master situations 112
takeover 111
Hilfe, Online- 73
Hochverfügbarkeit 104
aktiv-aktiv 104
aktiv-passiv 104
ARP-Anfragen 106
Cluster 104
Failover 104, 106
Heartbeat-Anfragen 16, 105
Hot-Standby 104
Knoten 104, 107
ID 107
Ressourcennutzung 108
Systemstatus 108
Linkbündelung 179
Linküberwachung 188
Live-Protokoll 108
Lizenzanforderungen 106
Status 43, 106-107
zurücksetzen 56
Systemanforderungen 106
Übernehame (Takeover) 105-106, 188
Home-Use-Lizenz 65
Anpassungen und 89
Homepage, Sophos UTM 69, 161
Hostname, System 60
DNS und 50
konfigurieren 50
Hot-Standby 104, 106
Knoten
Ressourcennutzung 108
Systemstatus 108
hot standby 109
autojoin 109
configuration of 108
of master 110, 112
deactivation of 111
Hotspots 456, 458, 469
access, unrestricted 469
cluster and 457
erstellen 459
in User Portal 83
Live-Protokoll 459
Rechtliche Hinweise 458
vouchers 468
Hotspots, Bereich im Benutzerportal 635
HTML rewriting, web application firewall 474
HTML5-VPN-Portal
Benutzerportal-Bereich 640
Fernzugriff 569-570
HTTP-Proxy *Siehe:* Webfilter
HTTP-Rückgabewerte 284
HTTPS
problems with 331
Rückgabewerte 284
WebAdmin-Zertifikat 59
WebAdmin CA-Zertifikat 59
WebAdmin CA certificate 24
HTTPS-Proxy*Siehe auch:* HTTP-Proxy; Webfilter
certificate authorities 329
fingerprint 333
problems with HTTPS 331
HTTPS-Proxy, Bereich im Benutzerportal 642

I

IANA 100
ICMP 262
Echo-Anfrage 263, 623
Echo-Antwort 263, 623
Flood-Schutz 278
konfigurieren 262
Icons *Siehe:* Symbole, WebAdmin
IDE-Controller 19
IDENT
IDENT-Verkehr und Firewall 259
Protokoll 293
IDENT-Relay *Siehe:* IDENT-Reverse-Proxy
IDENT-Reverse-Proxy 293
idle timeout, WebAdmin 62
IKE *Siehe:* Internet Key Exchange

improvement program, Sophos UTM 62
Informationen, weiterführende 15
Infosymbol 35
  Benutzerdefinitionen 126
  Dienstdefinitionen 122
  MAC-Adressdefinitionen 121
  Netzwerkdefinitionen 116
  Schnittstellendefinitionen 158
  Zeitraumdefinitionen 125
Inhaltsentfernung, Websiten
  deaktivieren 324
Initiale Anmeldeseite 23
Installation 15, 613
  abbrechen 19
  and basic configuration 22
  Dauer 22
  der Open-Source-Software 21
  des Enterprise-Toolkits 21
  Hardware-Anforderungen 15, 19
  Probleme nach 22
  Systemneustart nach 22
  Tastenbelegung während 18
  von CD-ROM 17
  Warnmeldung 21
Installationsanforderungen 16
Installationsanleitung 17
Installationsmenü 15
Instant-Messaging-Clients 291
Interface Address 116
Interface Broadcast Address 116
Interface Network Address 116
internal interfaces 26
internal mail server 27
interne Netzwerkkarte 20
interne Schnittstellen 20, 157
Internet (Netzwerkdefinition) 116, 157
Internet Explorer 16
Internet Key Exchange
  Authentifizierungsalgorithmen 524, 563
  Diffie-Hellman-Gruppen 524, 563
  SA-Lebensdauer 524, 563
  Verschlüsselungsalgorithmen 523, 563
Internet uplink, connection type 26
Internet, Zugriff 268
Internetnutzung, Berichte 590
Internetzeitserver *Siehe:* NTP-Server
Intrusion Prevention 274
  Angriffsmuster 274-275
  Berichte 255, 587, 589
  Ereignisse 255
  Flood-Schutz 276
  Live-Protokoll 275
  Portscan-Erkennung 278
  Schutz gegen DoS-Attacken 276
  settings of 27
  Signaturen 42
  Status 42
iOS-Konfiguration
  Cisco VPN Client 575-577
  L2TP 556
  PPTP 550
IP-Adressen
  aktive 72
  Aliasse 178
  Begrenzung von 72
  IPv6 206
  link-lokale, IPv6 208
  statische, für Benutzer über
    Fernzugriff 128
  zusätzliche 178
IP-Endpunkte, dynamische 118
IP-Header 518, 560
IP addresses
  blocking of 153
IP masquerading 26
IPS 42
  aktivieren 274
  Angriffsmuster 274-275
  Leistung 283
  Live-Protokoll 275
  Regeln 274, 276
    ändern 282
ipsec
  client installation instructions 561

high availability and 109
Verbindungen 560-562
IPsec 515, 557
Authentifizierung 520, 522, 527-528
X.509-Zertifikate 529, 567
Authentifizierungsalgorithmen 525, 565
Dead Peer Detection 529, 567
Dienstqualität (QoS) 201
ECN 522
Fehlersuche-Informationen 530, 568
IP-Pakete komprimieren 527, 566
L2TP über IPsec 552, 556
NAT-Traversal 517, 529, 559-560, 567
PFS-Gruppen 526, 565
PMTU 522
Probing von verteilten Schlüsseln 530, 568
Protokoll 511
Protokolle, verwendete 516, 558
Richtlinien 523, 527, 562, 566
SA-Lebensdauer 526, 565
strikte Richtlinie 526, 566
TOS-Bits 518, 560
Verbindungen 518, 520
Betriebsmodi 515, 557
entfernte Gateways 520, 522-523
Status 511
Verschlüsselung 516, 559
Verschlüsselungsalgorithmen 525, 564
XAUTH 523
Zertifikate
Informationen, enthaltene 50
Sperrlisten (CRLs) 530, 568
IPv6 206
aktivieren 207
Bridging und 191
IP-Adressen 208
IPv4 210
tunneln von 210
IPv4 und IPv6, gleichzeitig verwenden 165, 167, 178
link-lokale Adressen 208
Objektsymbole 207
Präfix-Bekanntmachungen 207
Präfix-Umnummerierung 209
Status 207
Tunnel-Broker 210
unterstützte Funktionen 206
IRC
Clients 291
Helfer für Verbindungsverfolgung 265

J

JavaScript 16
entfernen 324

K

Kennwort
Administrator- 55
für Shell 54
Loginuser- 55
einstellen 54
Root- 55
einstellen 54
von Benutzern
ändern 642
einstellen 127
zurücksetzen 55-56
Kennwortkomplexität 54
Kerberos-Authentifizierung 146-147
Kerberos authentication support 337
Kernelmodule 264
Knoten, Hochverfügbarkeit 104, 107
entfernen 108
herunterfahren 107
IDs 107
Master 107
neustarten 107
Slave 107
Status 107
Systemstatus 108
tote 105
überwachen 105
Version 107
Worker 107

Knowledgebase, Sophos 16-17, 28, 70, 96, 106, 166, 621-622
Known Issues List, Sophos UTM 621
Kommandozeilenzugriff 53, *Siehe auch:* Shell-Zugriff
Komplexität, Kennwort 54
Konfiguration 22
  des Systems 42
  des WebAdmin, Überblick 622
  von Up2Dates 75
  zurücksetzen 55
Konfigurations-Abbild, Support 626
Konfigurationsassistent *Siehe:* Assistent
Konsole *Siehe:* Shell-Zugriff
Kontaktdaten, Administrator 91

L

L2TP über IPsec 552, 556
  Client-Installationsanleitung 555
  Domänenname 577
  Fehlersuche-Informationen 556
  iOS-Konfiguration 556
  konfigurieren 552
  Zugriffskontrolle 554
LAG *Siehe:* Linkbündelung, Gruppen
LAN 157
Last, System 41
  reduzieren 615
Lastausgleich, Schnittstellen 104, 180, 231
Lastverteilung, Server 284
  Gewichtung 286
  Schnittstellenbindung 286
  Verteilungsregeln 284
  WAF-Server 471
LDAP 134, 141
  Backend-Server 141
  BaseDN 142
  Benutzerattribut 142
  Portnummer 141
LDAP browser 154
LDAP über SSL 137-138, 141
Lease-Tabelle, DHCP 248, 250
license 26
  for trial use 26
Liniendiagramme, Berichte 580
link-lokale Adressen, IPv6 208
Linkbündelung 179
  Alias-Schnittstellen 180
  Gruppen 179
Linküberwachung, Hochverfügbarkeit 188
Linux, SSH und 53
Listen 34
  Infosymbol 35
  suchen in 35
Live-Protokolle 33
Lizenz 41
  Ablauf 65
  Abonnements 64
  Aktivierungsschlüssel 65
  BasicGuard 69
  Basislizenz 71
  Benachrichtigung über 72
  erwerben 65
  FullGuard 66
  herunterladen 66
  hochladen 66
  hochstufen (Upgrade) 65
  Informationen zu 71
  installieren 71
  IP-Adressenbegrenzung 72
  kostenlose 72
  MSP 69
  Warnung 69
  zur privaten Nutzung 65
  zur Testnutzung 65
  zurücksetzen 56
Lizenzberechnung 72
Lizenzierung 64
  Support-Dienste 71
Lizenzschlüssel 17
load balancing, interfaces 109
load balancing, servers
  WAF servers 473

log files
deletion of 610
of SMTP 83
logging
local 609
thresholds of 610
notifications and 610
login page
initial 23
Standard 25
logins, failed 153
loginuser
Kennwort 55
Lokale Protokollierung 609
thresholds of 610

M

MAC-Adressdefinitionen
erstellen 121
Infosymbol 121
Mail-Manager 410
Datenbankprotokoll löschen 417
konfigurieren 417
Statistiken 415
Mail-Manager-Fenster 410
deletion of emails 412
download of emails 412
false positives, report of 412
global cleanup actions 412
öffnen 415
POP3 quarantine 411
release of emails 412
restrictions of users 412
SMTP-Protokoll 414-415
SMTP-Spool 412
SMTP quarantine 411
Mail-Protokoll, Bereich im Benutzerportal 632
Mail-Quarantäne*Siehe auch:* E-Mail-Quarantäne
Benutzerportal-Bereich 630
Mail Protection *Siehe:* Email Protection
mail server, internal 27
Mailserver, interner 349, 351
Management Information Base, SNMP 97
Manager (Benutzerrecht) 59
Maskierung (Masquerading) 26, 267, 290
Regeln 267
Master (HA-Knoten) 105, 107
Master (high availability node) 109
MD5-Authentifizierung, OSPF 221
MD5 (Hash-Algorithmus) 516, 558
Menü, WebAdmin 32
Suchfeld 33
Mesh-Netzwerke 453
MGE-UPS-Systeme (Hersteller) 17
MIB *Siehe:* Management Information Base, SNMP
Microsoft Active Directory *Siehe:* Active Directory
MIME-Typen
blockieren 310
deaktivieren 324
der PAC-Datei 335
filtern 354
MIME Type (Web Filter message) 92
MIME types
Blacklist 374
blocking of 334
filtering of 374
Whitelist 374
Modem (PPP) (Schnittstelle) 160, 175
MTU 177
monitoring
of requests, web application firewall 477
MSCHAPv2 (Authentifizierungsprotokoll) 548
MSP-Lizenz 69
MTU
3G/UMTS 163
DSL (PPPoA/PPTP) 174
DSL (PPPoE) 171
Ethernet-DHCP 169
Ethernet-Statisch 165
Ethernet-VLAN 167
Modem (PPP) 177

Multicast-Gruppen 119, 234
  Präfixe 234
Multicast Routing 231
  aktivieren 232
  deaktivieren 233
  Einstellungen, erweiterte 236
  Fehlersuche-Informationen 236
  Firewallregeln, automatische 236
  IP-Adressbereich 232
  kürzester Pfad 236
  Live-Protokoll 233
  Rendezvous-Point-Router 234
  Routen 235
  Schnittstellen 233
Multicast, Hochverfügbarkeit 105
Multilink, DSL (PPPoE) 172
Multipath-Regeln, Uplink-Ausgleich 184
MyUTM Portal 65, 70, 623

N

Nachbarrouter, BGP 225
NAS-Kennungen, RADIUS 144-145
NAT 178, 266
  1:1 NAT 268, 270
  DNAT 268
  Firewall und 259
  Firewallregeln, automatische 271
  Maskierung (Masquerading) 267
  Regeln 269
  SNAT 268
  Volles NAT 270
NAT-Traversal 517, 529, 559-560, 567
netstat 625
Network Protection 255-256, 258-268, 272-278, 280-284, 286-287, 289-291, 293
  Abonnement 71
  Advanced Threat Protection 42, 272
  Ausnahmen bei 280
  Berichte 586-587
  Country-Blocking 260
    Ausnahmen 261
  Firewall 255
  generischer Proxy 290
  ICMP 262
  IDENT-Reverse-Proxy 293
  Intrusion Prevention 274, 278
  NAT 266, 268
  Server-Lastverteilung 284
  SOCKS-Proxy 291
  Statistiken 255
networks
  never blocked 153
Netzmaske 119
Netzwerkaktivitäten 579
Netzwerkdefinitionen
  an Schnittstelle knüpfen 120
  Arten 117
  DNS-Gruppen 119
  DNS-Hosts 118
  erstellen 117
  Hosts 117
  Infosymbol 116
  Internet 116
  Multicast-Gruppen 119
  Netzwerkgruppen 119
  Verfügbarkeitsgruppen 119
Netzwerkdienste 237
  DNS 237
  NTP 254
Netzwerke 116
  definieren 115-116
  externe 157
  RED *Siehe:* RED-Verwaltung
  statische 116
  WLAN *Siehe:* WLAN-Netzwerke
Netzwerkgruppen 119
  namens „Uplink Primary Addresses“ 184
Netzwerkkarten 16, 19
  Datenübertragungsrate 42
  erkennen 157
    Software-Appliance und 157
  Flow-Monitor 42, 45
  Heartbeat-fähig 16, 106
  interne 20

konfigurieren 158
Name 42
Reihenfolge 22
Status 42
SysIDs 164, 169
Netzwerkmaske *Siehe:* Netzmaske
Netzwerknutzung, Berichte 105, 584-585
Netzwerkschnittstellen *Siehe:* Schnittstellen
Netzwerksichtbarkeit, Application Control 42, 340
Netzwerkstatistiken 625
Übersicht 157
Netzwerküberwachung 97
Uplink-Überwachung 202
Netzwerkverkehrsdaten, Berichte 105
Neuigkeiten, Sophos News Feed 44
Neustart, System 112
manuell 112
nach Installation 22
NIC-Bonding *Siehe:* Linkbündelung
nodes, high availability
Master 109
Notifier MIB von Sophos, SNMP 99
Novell eDirectory *Siehe:* eDirectory
NTLMv2-Support 146
NTP 254
NTP-Server 50, 52, 254
testen 53

O

Object Identifier, SNMP-Traps 100
Objektleisten 40
Tastaturkürzel 61

Ö

öffentliche Schlüssel, OpenPGP 396
öffentliche Schlüssel, SSH DSA 613
OID, SNMP-Traps 100
one-time passwords 148
Benutzerportal 84, 629, 638
settings of 149, 152
user configuration 638
one-time token 148
Onlinehilfe, Aktualisierung 73
Open-Source-Software installieren 21
OpenPGP-Verschlüsselung 391, 396
öffentliche Schlüssel 396
Schlüsselserver 391
Operating Instructions 15
operation modes
bridge mode 22
routing mode 22
organisatorische Informationen, System 50
OSPF 213, 215
aktivieren 216
Bereiche 217
deaktivieren 216
Fehlersuche-Informationen 221
Live-Protokoll 219-220
MD5-Authentifizierung 221
Prüfsummenschlüssel 221
Schnittstellen 219
settings, advanced 222
OTP *Siehe:* one-time passwords
Outlook 404
add-in 404
Outlook Anywhere
web application firewall, passing of 477
Outlook Web Access 482

P

PAC-Dateien
Beispiel 335
MIME-Typ 335
PAC files 335
packet flow 22
packets
dropping of 273
Pakete
abgelehnte 41
verwerfen 274
verworfene 41, 255
Paketverlust 263, 623

Partitionsauslastung 583
Protokollpartition 583
Root-Partition 41, 108, 583
Speicherpartition 583
Partnerportal, Sophos NSG 623
password
of administrator 25
setting of 24
of users
change of 84
of WebAdmin 25
password complexity 153
password guessing 153
Pattern-Aktualisierungen 72
herunterladen 75-76
installieren 73, 75-76
Onlinehilfe 73
Patternversion 41, 75
PCI-ID 22
PDF (Format)
Berichtsdaten herunterladen in 586, 588-590, 592, 596, 601-603, 606, 608
Peer-Router *Siehe:* Border Gateway Protocol, Neighbor-Router
PEM (Dateiformat) 396, 538
PIM-SM *Siehe:* Multicast Routing
Ping 623
konfigurieren 263
Ping-Prüfung 22, 623
Server-Lastverteilung 285
Verfügbarkeitsgruppe 119
PKCS#12-Container (Dateiformat) 538
PMTU 522
POP3-Konten 83
POP3-Konten, Bereich im Benutzerportal 633
POP3-Meldungen, Anpassung von 90
POP3-Proxy 375
aktivieren 376
Antispam-Mechanismus 378
Ausdruckfilter 379
E-Mail-Adressen auf Blacklist 379, 634
E-Mail-Adressen auf Whitelist 405, 633
Spam-Kennzeichnung 379
Spamfilter 378
Antiviren-Mechanismus 377
Email Encryption 389
maximale E-Mail-Größe 377
unscannbare E-Mails 377
verschlüsselte E-Mails 377
Ausnahmen 380
Ausnahmenliste, Transparenzmodus 381
Dateierweiterungenfilter 378
E-Mails löschen 376, 384
konfigurieren 376
Live-Protokoll 377
Portnummer 375
Quarantänebericht 407
Server 381
Status 42
TLS 385
vorabholen 383, 405
Zeichensätze 385
Zeitüberschreitungseinstellungen, Client 376
POP3-Quarantäne *Siehe:* E-Mail-Quarantäne
POP3-Server
definieren 381
TLS 382
POP3 Message Blocked (POP3 proxy message) 97
POP3 proxy 27
antispam engine
blacklisting of email addresses 83
whitelisting of email addresses 83
messages of, customization 97
POP3 servers
allowed 83
Port Forwarder *Siehe:* generischer Proxy
port number
of WebAdmin 23
Port Trunking *Siehe:* Linkbündelung

Portnummer
der SUM-Kommunikation 103
des Benutzerportals 85
des POP3-Proxys 375
des Quarantäneberichts 409
des SUM-Gateway-Managers 103
des SUM-WebAdmins 103
von Active Directory 138
von eDirectory 137
von LDAP 141
von RADIUS 143, 441
von SSH 54
von TACACS+ 146
Portscan-Erkennung, Angriffschutz 278
aktivieren 279
PPTP 548-551
aktivieren 548
Client-Installationsanleitung 549
DNAT und 268
Domänenname 577
Fehlersuche-Informationen 551
Helfer für Verbindungsverfolgung 265
iOS-Konfiguration 550
Live-Protokoll 550
Verschlüsselung 551
Präfix-Bekanntmachungen, IPv6 207
DHCP-Leases und 250
prefetching, authentication
Gruppen 154
interval of 154
time of 154
with Active Directory 154
with eDirectory 154
Probleme, nach Installation 22
Profile, Webfilter 314
Filteraktionen 310-312
policy test 338
übergeordnete Proxies 322
profiles, SMTP proxy 370-375
Allgemein 375
profiles, Web Filter 314
Filteraktionen 306, 322
Protokolldateien
ansehen 581
Archiv 581, 612
E-Mail 613
FTP-Server 612
SMB-Freigabe 612
SSH-Server 613
herunterladen 581
heutige 581
Live-Protokoll 581
löschen 581-582
SMTP 632
suchen in 581-582
zurücksetzen 56
Protokolle
AH 516, 558
ESP 516, 558
IPsec 511
LDAP 141
MSCHAPv2 548
NTP 254
RADIUS 143
Routing- 213
Syslog 611
TACACS+ 145
Protokollierung 44, 579
besuchte Webseiten 325
blockierte Webseiten 325
entfernte 610
konfigurieren 50, 609
Syslog verwenden 610
Zeiteinstellungen 50
Zeitlücken 51
Protokollpartition
Histogramm, Belegung 579
Speicherplatzbelegung 41, 108
Status 579
Proxies
FTP 344
generischer Proxy 290
HTTP/S 296
IDENT-Reverse- 293

POP3 375
Reverse-Proxy *Siehe:* Web Application Firewall
SMTP 349
SOCKS 291
Webfilter 296
Proxy-ARP (Funktion)
bei Ethernet-Statisch 165
bei Ethernet-VLAN 167
Proxy-Server, staatlich kontrolliert *Siehe:* übergeordnete Proxies
Prozessliste, Support 625
Prozessor 19
Systemanforderungen 16
Prüfsummenschlüssel, OSPF 221
ps (Support-Tool) 625
public keys, S/MIME 394-395

Q

Quality of Service *Siehe:* Dienstqualität (QoS)
Quarantäne-E-Mails
Fehlfunde 405
freigeben 405-406, 630
Nutzerbeschränkung 409, 632
zugelassene Netzwerke 409
löschen
vom Server 384
Quarantäne-Statusmeldungen
anpassen 90
Quarantänebericht 83, 127, 405-409, 633
activation of 406
anpassen 90
Ausnahmen 407
delivery time 407
E-Mails freigeben 405-406
Nutzerbeschränkung 409
zugelassene Netzwerke 409
Fehlfunde 405
Hostname 409
HTML and 407
message text, customization of 407
Portnummer 409
report, additional 407
Verteilerlisten 407
Whitelist 405
quarantined emails 82
deletion of 412
download of 412
false positives
report of 412
release of 83, 412
restrictions of users 412
Quick Start Guide Hardware 15

R

RADIUS 134, 143
Backend-Server 143, 441
NAS-Kennungen 144-145
Portnummer 143, 441
Protokoll 143
vereinbarter Schlüssel 144, 441
RAID
Anzeige auf Dashboard 17
Controller 17
Unterstützung 17
RAM
Speicherplatzbelegung 41, 108
Systemanforderungen 16
RBLs 357, 372
extra 372
RDNS-Einträge, fehlende 359
RDNS entries, missing 372
readonly (Benutzerrolle) 58
Rechte, von Benutzern 59
recipient verification, SMTP proxy 371
RED-Appliances 493
konfigurieren 493-494
Live-Protokoll 494
RED-Verwaltung 493-494, 496, 500, 504-508
activation of 494
einrichten 493-494
Übersicht 494
Einrichtungshilfe 496, 506-508

failover uplink 503
Live-Protokoll 494
Routing 493
settings, global 494
Status 42
UTM als Client 508
UTM as client 496
UTM as host 496
RED appliances
automatic deauthorization 495
bridging of 508
configuration of 496-497, 500, 504-506
deletion of 506
DHCP servers 506-507
Einrichtungshilfe 496, 506-508
operation modes 499, 506-508
unlock code 497, 505
uplink modes 498, 508
VLAN 500
RED hub 494, 496
configuration of 495
RED Provisioning Service 495, 504
redundancy, computer networks 109
Redundanz, Computer-Netzwerke 104, 179
REF_ auflösen 626
reguläre Ausdrücke 35
Relative Distinguished Name 139
Relays, DHCP 247
Relays, E-Mail 365-366
Antiviren-Scan 366
Authentifizierung 365
Blacklist 366
hostbasierte 365
Upstream-Hosts 365
Remote-Syslog-Server 610
Remote Ethernet Device *Siehe:* RED-Verwaltung
Rendezvous-Point-Router, Multicast Routing 234
Repeater, WLAN 454
Ressourcennutzung 41, 104
restoration, backups 25
Reverse-DNS 118
Reverse-Proxy *Siehe:* Web Application Firewall
Richtlinienrouten 212, 214
Root-DNS-Server 238
Root-Kennwort 55
Route Flapping 213
Routemaps, BGP 227
Routing
Anfragerouten 239
automatische 212
BGP 224
Multicast Routing 231
Richtlinienrouten 212, 214
statische Routen 212
statisches Routing 212
Routing-Protokolle 213
Routing-Schleifen 213
Routing-Tabelle 212, 214, 625
routing mode 22
RPS *Siehe:* RED Provisioning Service
RSA-Schlüssel
Site-to-Site-VPN IPsec 527-528
und Backups 78
Rückgabewerte, HTTP/S 284

S

S/MIME-Verschlüsselung
Zertifikate 395
automatisch extrahieren 391
S/MIME encryption
authorities 394
public keys 394-395
scannen *Siehe:* Antiviren-Mechanismus, scannen
Schaltflächen, WebAdmin 38
Schieberegler, im WebAdmin 38
Schlüssel
für Cookie-Signierung 486
für URL-Hardening 486
Schlüsselserver, OpenPGP 391

Schnittstellen 157
administrative 20
Aliasse 180
Arten 159, 162, 164, 166, 168, 170, 173, 175, 178
3G/UMTS 159, 162
DSL (PPPoA/PPTP) 160, 173
DSL (PPPoE) 160, 170
Ethernet-DHCP 160, 168
Ethernet-Statisch 160, 164
Ethernet-VLAN 160, 166
Gruppe 159, 161
Modem (PPP) 160, 175
automatische Adressaushandlung 187
automatische Definitionen 159
dynamische Adresszuweisung 159
default gateway 26
Dienstqualität (QoS) 191, 201
dynamisches Routing 215
external 26
externe 157, 164, 169
Flow-Monitor 42, 45
Gruppen 159, 161
Infosymbol 158
internal 26
interne 20, 157
konfigurieren 157
Lastverteilung 104, 180
Linkbündelung 179
load balancing 109
mit Status „An“ 164, 166, 168, 170, 173, 175, 178
mit Status „Aus“ 159, 164, 166, 168, 170, 173, 175, 178
Multicast Routing 233
namens „Internal“ 159
OSPF 215
Slotinformation 161
Tabelle 626
Uplink-Ausgleich 180
Uplink-Überwachung 202
virtuelle 158, 179, 184
Schnittstellenbindung
Server-Lastverteilung 286
Uplink-Ausgleich 182
SCP-Server 613
SCSI-Controller 19
Secure Copy, Archivierungsmethode 613
Secure Shell 53, *Siehe auch:* SSH
security warning, web browser 23, 25
Seitenumbruch, Tabellen 61
self-signed certificate
of system 23
Sender Policy Framework *Siehe:* Antispam-Mechanismus, SPF-Prüfung
Server
DHCP 26, 244
DNS 237
für Authentifizierung 136
mail, internal 27
NTP 254
SCP 613
Server-Lastverteilung 284
Gewichtung 286
Ping-Prüfung 285
Schnittstellenbindung 286
Verteilungsregeln 284
Server Error (Web Filter message) 93
services
allowed by Web Filter 334
types of 27
SHA-1 (Hash-Algorithmus) 516, 558
Shell-Zugriff 53
Kennwörter einrichten 54, 56
nach Kennwortzurücksetzung 56
shutdown, system
logging thresholds and 610
Sicherheitsbedrohungen 41
identifizieren 579
Sicherheitswarnung, Webbrowser 59-60
Sicherheitszertifikat *Siehe:* Zertifikate
Signaturen, Intrusion Prevention 42, 274
signierende CA 539
für VPN 541

Simple Network Management
  Protocol *Siehe:* SNMP
Single Sign-On 146
  von Active Directory 135, 146
  von eDirectory 147
SIP 287
  Helfer für Verbindungsverfolgung 287
Site-to-Site-VPN 511
  Amazon VPC 512
  certificates for 24
  entfernte Gateways 520, 522-523
  IPsec 515
  SSL 531, 534-535
  Status 43, 511
Sitzungen, WebAdmin, Übersicht 49
skiplist
  Webfilter 335
Slave (HA-Knoten) 105, 107
Slotinformation, Schnittstellen 161
Smarthosts
  Benachrichtigungen und 88
  SMTP-Proxy 370
SMB-Freigabe als Protokollarchiv 612
SMTP
  data protection 361
SMTP-Protokoll 414-415
  im Benutzerportal 632
SMTP-Proxy
  aktivieren 350
  Antispam-Mechanismus 356
    Ausdruckfilter 358
    BATV 360, 369
    E-Mail-Adressen auf Blacklist 358, 634
    E-Mail-Adressen auf Whitelist 405, 633
    Greylisting 359
    RBLs 357
    Spam-Kennzeichnung 358
    Spamfilter 357
    SPF-Prüfung 360
  antispam engine
    Ausdruckfilter 374
    BATV 372
    blacklisting of email addresses 83, 373
    greylisting 372
    RBLs 372
    Spamfilter 373
    SPF check 372
    whitelisting of email addresses 83
  Antiviren-Mechanismus 352-353
    E-Mail-Fußzeile 355
    unscannbare E-Mails 353
    verschlüsselte E-Mails 353
  antivirus engine 373
    encrypted emails 373
    unscannable emails 373
  Ausnahmen 363
  Betriebsmodi 350
    einfach 350
    Profil 350
    transparent 367
  certificate authorities
    fingerprint 395
  data protection 375
  Dateierweiterungenfilter 355, 374
  DKIM 368
  E-Mail-Relays 365-366
  Einschränkungen, Einstellungen 369
  Empfängerverifizierung 352, 361, 371
  Fußzeilenformat 369
  konfigurieren 349-350
  maximale E-Mail-Größe 369
  messages of, customization 97
  MIME
    Blacklist 374
  MIME-Typ-Filter 354, 374
  MIME type Whitelist 374
  Postmaster-Adresse 369
  Profile 370, 375
    Allgemein 375
    Ausdruckfilter 374
    BATV 372
    blacklisting 373-374
    Empfängerverifizierung 371
    extension filter 374

MIME
type filter 374
RBLs 372
Routing 371
scanning of emails 373
Spamfilter 373
unscannable emails 373
Vertraulichkeitsfußzeile 374
Routing 350, 371
Smarthosts 370
SMTP-Hostname 369
SPX template 375
Status 42
TLS 367
übergeordnete Proxies 366
Vertraulichkeitsfußzeile 368, 374
whitelisting 374
SMTP-Quarantäne *Siehe:* E-Mail-Quarantäne
SMTP-Spool 412
E-Mails abweisen (bounce) 413
E-Mails herunterladen 413
E-Mails löschen 413
globale Aufräumaktionen 414
Zustellungsversuche, erzwungen 413
SMTP domains 27
SMTP relay 27
SMTP, Email Encryption 389
SNAT 268
Firewall und 259
Maskierung (Masquerading) 267
SNMP 97
Agent 99
Anfragen 97-98
Community-String 99, 101
Fehlercodes 100
Geräteinformationen 99
Sophos Notifier MIB 99
Traps 87, 97, 100
SOCKS-Proxy 291
Benutzerauthentifizierung 292
Bind-Anfragen 292
Hostname-Auflösung und 292
Protokollversionen 292
Software, vorinstalliert 15
Sommerzeit 51
Sophos' Portal *Siehe:* MyUTM Portal
Sophos Authentication Agent 132-133
Sophos Knowledgebase 16-17, 28, 70, 96, 106, 166, 621-622
Sophos Newsfeed 44
Sophos NSG Partnerportal 623
Sophos NSG Supportforum 28, 70
Sophos RED Provisioning Service *Siehe:* RED Provisioning Service
Sophos User Authentication 135-136
Live-Protokoll 136
Sophos UTM-Benutzerportal *Siehe:* Benutzerportal
Sophos UTM FTP-Server 76
Sophos UTM Homepage 69, 161
Sophos UTM improvement program 62
Sophos UTM Manager, Status von 43
Sophos UTM Portal 65
Sophos UTM Up2Date-Blog 70, 621
Source Network Address Translation *Siehe:* SNAT
Spam-E-Mails, blockiert 42
Spam-Kennzeichnung 358, 379
Spamfilter 357, 373, 378
Spanning Tree Protocol 191
Sperrdateien und Backups 79
Sperrlisten (CRLs) 491-492, 536, 540, 577-578
SPF-Prüfung, SMTP-Proxy 360
SPF check, SMTP proxy 372
Split-Tunneling 545
Sprache, WebAdmin 57
SPX encryption
Outlook add-in 404
Spyware *Siehe:* Antispyware-Mechanismus
SQL-Injections, Schutz vor 471
SQL injections, protection from 481

SSH 53
  Authentifizierungsmethode 53
  Clients 53, 291
  Lausch-Port für Daemon 54
  Linux und 53
  öffentliche Schlüssel 54
  Portnummer 54
  Zugriffskontrolle 53
SSH-DSA-Schlüssel 613
  Backups und 613
  öffentliche 613
SSH-Server als Protokollarchiv 613
SSL
  LDAP über 137-138, 141
SSL-Scans
  deaktivieren 324
  transparenter Proxy und 324
SSL-VPN, clientlos 569
SSL-VPN, Fernzugriff 544, 546
  aktivieren 544
  Client-Installationsanleitung 545
  Client-Software 544
  Konfigurationsdateien für Benutzer 544
  konfigurieren 546-548
  Live-Protokoll 546
  Profile 544
  Split-Tunneling 545
  Zertifikate 544
SSL-VPN, Site-to-Site 534-536
  Konfiguration 531
    Server 531, 533
    von Clients 533-534
  konfigurieren 534-536
  Status 511
  transparenter Webfilter und SSL-Scans 531
  Verbindungen 532-533
SSL-Zertifikate 544
  Kennungen 135
  von Benutzern 135
SSO *Siehe:* Single Sign-On
standard (Web Filter operation mode) 300
Standort, Systemeinstellungen 20
statische Routen 212
statische Zuordnungen, DHCP 248
statische Zuordnungen, DNS 240
statisches Routing 212
statistic overview
  of emails 349
statistischer Überblick
  des Netzwerks 157
  über Network-Protection-Ereignisse 255
  über Web-Surfing 295
  von E-Mails 415
Status
  operating, of system 28
  Protokollpartition 579
  System 41
Störung, Hardware, Umgang mit 104
streaming content 337
Subnetz 20
Suchfeld, des Menüs 32
  Tastaturkürzel 61
Suchmaschinen 595
SUM 101
  Funktionsfähigkeit 103
  Live-Protokoll 104
  Server 103
  Verbindungsstatus 103
SUM-Objekte 103
  entfernen 104
  lokale Kopien 104
SUM-Server
  als Up2Date-Cache 102
  authentifizieren an 102
  Privilegien 102
  Rechte 102
  Status 43
SUM Gateway Manager
  Portnummer 103
SUM WebAdmin
  Portnummer 103
SuperAdmins (Benutzergruppe) 128-129

Support 28, 621
  contact information 97
  Konfigurations-Abbild 626
  Kontaktinformationen 622
  REF_ auflösen 626
  Sophos NSG Partnerportal 623
Support-Dienste 71, 622
Support-Stufen 622
Support-Tools 623
  DNS-Lookup 623
  IP 625
  netstat 625
  Ping 623
  ps 625
  Traceroute 623-624
support tools
  DNS-Lookup 624
Support, Sophos UTM 622
Supportfälle 623
Supportforum, Sophos NSG 28, 70
Surf Protection (Web Filter message) 91
Swap-Auslastung 108, 583
Switches
  HA-Anforderungen 106
  Systemanforderungen 16
Symbole, WebAdmin 38
  Access-Point-Symbole 455
  Infosymbol 35
  IPv4/IPv6-Symbole 207
Symbolleiste, WebAdmin 33
SYN-Flood-Schutz 277
synchronization, Active Directory Group Membership 155
SysIDs, Netzwerkkarten 164, 169
Syslog-Protokoll 611
Syslog-Server
  entfernte 610
  Protokollauswahl 611
  Puffergröße 611
system
  settings of 22, 27
  status of 28
System
  herunterfahren 112
    nach Werkszurücksetzung 55-56
  konfigurieren 15, 42, 50
    zurücksetzen 56
  neustarten
    manuell 112
    nach Installation 22
  organisatorische Informationen 50
  vorinstalliert 15
system ID, reset of 56
Systemanforderungen 16
Systemlast 41
  reduzieren 615
Systemmeldungen
  anpassen 89

T

Tabelle
  Routing-Tabelle 212, 214, 625
  Schnittstellen 626
Tabellen *Siehe auch:* Listen
  Daten sortieren 586, 588-590, 600, 602-603, 606, 608
  Seitenumbruch 61
TACACS+ 134, 145
  Backend-Server 145
  Portnummer 146
  Schlüssel für Authentifizierung/Verschlüsselung 146
Tags, VLAN 166
Tastatur-Layout, auswählen 19
Tastaturkürzel, WebAdmin 61
Tastenbelegung, während der Installation 18
Telnet, Clients 291
terms of use, WebAdmin 62
TFTP, Helfer für Verbindungsverfolgung 265
Time-to-live (TTL) 118
timeout, authentication 334
timeout, WebAdmin 62
TLS, POP3-Proxy 382, 385
TLS, SMTP-Proxy 367

tools, support
DNS-Lookup 624
Tools, Support 623
DNS-Lookup 623
IP 625
netstat 625
Ping 623
ps 625
Traceroute 623-624
Tortendiagramme, Berichte 580
TOS-Bits 518, 560
Traceroute 623-624
konfigurieren 263
Transparent (SMTP-Proxy-Modus) 367
Ausnahmen 367
transparent (Web Filter operation mode) 302
full transparent 303
skiplist 335
Transparent (Webfilter-Betriebsmodus) 317
SSL-Scans und 324
volltransparent 319
Traps, SNMP 100
trial license 26
TTL *Siehe:* Time-to-live (TTL)
Tunnel-Broker, IPv6 210
types of services 27

Ü

übergeordnete Proxies
als Up2Date-Cache 76-77, 102
authentifizieren an 77, 367
SMTP-Proxy und 366
Webfilter und 313, 322
Übernahme, Hochverfügbarkeit 105-106, 188
Übersetzen, Systemmeldungen 89
Überwachung
der Knoten, Hochverfügbarkeit 105
des Netzwerks 97
des Uplinks 202
des Verbindungsstatus, Hochverfügbarkeit 188
von Systemen 101

U

UDP-Flood-Schutz 278
UMTS (Schnittstelle) 159, 162
unterbrechungsfreie Stromversorgung 17
Batteriebetrieb 17
Benachrichtigungen und 17
erkennen 17
Status 41, 108
USB-Ports 16
Unternehmenslogo anpassen 90
Unternehmenstext anpassen 91
Up2Date-Blog, Sophos UTM 70, 621
Up2Date-Cache 76
übergeordnete Proxies 76-77
Up2Date-Information, Sophos UTM 70, 621
Up2Dates 72
digitale Signatur 72
Firmware- 74
herunterladen 73-74
installieren 73-74
automatische 75
konfigurieren 75
manuell hochladen 76
Pakete zurücksetzen 56
Pattern- 75
planen 74
System-Backup, automatisches und 73
Update-Server 73
Verbindungsprobleme 73
Update-Server 73
Upgrades, der Lizenzen 65
Uplink-Ausgleich 180
Gewichtung 181
Multipathregeln 184
Schnittstellenbindung 182
überwachen 182
Uplink-Überwachung 202
Aktionen 203
aktivieren 202
automatische 204

deaktivieren 202
Uplink Interfaces (virtuelle Schnittstelle) 184
Uplink Primary Addresses (Netzwerkgruppe) 184
Uplink, Backup- 180
uplink, Internet (connection type) 26
uploads, antivirus scanning 479
URL-Filter
blockierte URLs 42
deaktivieren 324
URL-Hardening 478, 482
entry URLs 478
Outlook Web Access 482
Schlüssel 486
URL filter
Kategorien 328
URL rewriting, web application firewall 474
USB-Port, Systemanforderungen 16
USV *Siehe:* unterbrechungsfreie Stromversorgung
UTC 51
UTM ID, reset of 56

V

VDSL 170
Verbindungen, Beenden von 274
Verfügbarkeitsgruppen 119
immer aufgelöst 120
Überwachungsintervall 120
Verifizierungs-CA 539
Verkehrskennzeichner, Dienstqualität 47-48, 193
Zuordnung 201
Verschlüsselung, E-Mail *Siehe:* Email Encryption
Verschlüsselung, WLAN-Netzwerke
WEP 442-443
WPA/WPA2 Personal 440, 442
Verschlüsselungsalgorithmen
3DES 517, 559
AES 444, 517, 559
Internet Key Exchange 523, 563
IPsec 525, 564
TKIP & AES 444
Version 41
Firmware- 41
Pattern- 41
Verteilerlisten 407
Whitelist 408
Verteilungsregeln, Server-Lastverteilung 284
Vertraulichkeitsfußzeile, SMTP-Proxy 368
Verwaltung, zentrale, der UTM 101
Verzeichnisdienste 136
Active Directory 138
eDirectory 136
LDAP 141
RADIUS 143
TACACS+ 145
video content, filtering 374
Videoinhalt filtern 354
Viren*Siehe auch:* Antiviren-Mechanismus
blockiert 41
virtuelle Schnittstellen 158, 179
MAC-Adressänderungen 189
namens „Uplink Interfaces“ 184
virtuelle Webserver
entsprechende echte Webserver 471
Virtuelle Webserver 471, 474-475
disabling compression support 473
HTML rewriting 474
matching real webservers 473
URL rewriting 474
virtuelles LAN *Siehe:* VLAN
Virus Detected (Web Filter message) 92
Virus Scan in Progress (Web Filter message) 92
VLAN 166
RED appliances 500
Switche konfigurieren 158
tags 450
Tags 166, 452
WLAN-Netzwerke
activation of 450
aktivieren 452

IDs 451-452
tagging 451
tags 451
Tags 452
Voice over IP *Siehe:* VoIP
VoIP 287
H.323 289
SIP 287
Vollständig qualifizierter Domänenname *Siehe:* FQDN
volltransparent (Webfilter-Betriebsmodus) 319
Vorabholen, POP3-Proxy 383, 405
vorinstallierte Software 15
vorinstalliertes System 15
Vorlagen
Backup-Vorlagen 80
Web-Vorlagen 95
vouchers, wireless hotspots
creation of 468
deletion of 469
in User Portal 83
VPN 511, 543, *Siehe auch:* Site-to-Site-VPN; Fernzugriff
signierende CA 541

W

WAF *Siehe:* Web Application Firewall
Warnmeldung, bei der Installation 21
Wartungsvertragsstufe, Support 622
Web-Meldungen 91
administrator information 93
Application Control 92
Blacklist 91
Bypass Content Block 93
Dateierweiterung 92
Download Complete 92
Download in Progress 92
E-Mail-Adresse 93
File Size 92
MIME-Typ 92
modification of 93
Server Error 93
Surf Protection 91
Transparent Mode Authentication 92
Virus Detected 92
Virus Scan in Progress 92
Web-Surfing 295
Datensammlung 295
Web-Vorlagen 95
anpassen 95
hochladen 96
Web Application Firewall 471, 473, 475-477, 482-484, 486-487, 490-491
antivirus engine 479
Ausnahmen 483-484
authentication form templates 491
authentication profiles 487
Authentifizierung 487
Berichte 607
Cookie-Signierung 478, 486
cross-site scripting filter 481
echte Webserver 471, 475-476
Echte Webserver 473
Form-Hardening 479, 482
Form Hardening 486
HTML-Umschreibung 483
HTML rewriting 474
konfigurieren 486
Lastverteilung zwischen Servern 471
monitoring of requests 477
Outlook Anywhere 477
Outlook Web Access 482
Profile 476, 482
rejection of requests 477
Site-Path-Routing 484, 486
SQL injection filter 481
Status 43
URL-Hardening 478, 482, 486
URL rewriting 474
virtuelle Webserver 471
Virtuelle Webserver 471, 474-475
Webserver Protection 477, 480
Zertifikatverwaltung 491

web browser
certificates and 23
Kerberos authentication support 337
security warning 23, 25
Web Filter configuration, automatic 335
Web Protection 44, 295-296, 300, 303-304, 306, 310-312, 314, 318, 321-327, 329-333, 335-338, 344-347
Abonnement 71
Application Control 339
Berichte 590, 601
policy test 338
settings of 27
Statistiken 295
Status 295
Web Surfing (Dienstdefinition) 440
webadmin
administrators 25
certificate of 24
Nutzungsbedingungen 62
password for 25
port number 23, 62
protocol of 23
timeout of 62
WebAdmin 15, 31
Administratoren 57
Benutzerrollen 58
Browser, Registertitel 61
Dashboard 32, 41
Dialogfenster 37
Konfiguration, Überblick 622
konfigurieren 57
Änderungen überwachen 49
Listen 34
Menü 32
Objektleisten 40
Schaltflächen 38
Sitzungen, Übersicht 49
Sprache auswählen 57
Symbole 38
Symbolleiste 33
Tastaturkürzel 61
Version 41
Zertifikat 60
Informationen, enthaltene 50
Zugriffskontrolle 57-58
Zugriffsverkehr protokollieren 58
Webbrowser
HTTP-Proxy-Konfiguration, automatische 246
Kerberos-Authentifizierung 146-147
NTLMv2-Support 146
Sicherheitswarnung 59-60
Systemanforderungen 16
Webfilter 296
activation of 300
administrator information 93
Antiviren-Mechanismus 311, 324
Ausnahmen 323, 325-326, 333
Standardmodus und 324
authentication at 334
authentication modes 301, 303
Apple OpenDirectory SSO 337
authentifizieren an 324
Single Sign-On verwenden 146
Authentifizierungsmodi 319
Benutzer umgehen 327
Betriebsmodi
Standard- 324
transparent 317
volltransparent 319
blockieren
Dateierweiterungen 310, 324
Download-Größe 324
MIME-Typen 310, 324
URLs 324
Website-Kategorien 295
blocking
download size 92
encrypted files 334
MIME types 334
spyware 307
unscannable files 334
website categories 27, 307, 328

websites 307
CA-Zertifikat 642
CA certificate 84
cache 336
Cache 324
zurücksetzen 56
categorization parent proxy 336
configuration of 300
deactivation of 300
DNS requests 334
Download-Größe 324
Download-Verwaltung 93, 334
Filtering Options 323
Inhaltsentfernung 311, 324
konfigurieren 314
Live-Protokoll 304
maximum scanning size 311
Meldungen 50
anpassen 90
messages
modification of 91
operation modes 300
full transparent 303
Standard 300
transparent 302
transparent with authentication 92
policy test 338
port number 334
Profile 314
Filteraktionen 306, 310-312, 322
Protokollierung 590
besuchte Seiten 313, 325
blockierte Seiten 313, 325
Richtlinien 304
testen 338
SafeSearch 312
skiplist, transparent mode 335
SSL-Scans 324
Status 42
streaming content 337
target services 334
übergeordnete Proxies 313, 322
URLs, ungültige 591
web browser configuration, automatic 335
Webbrowser-Konfiguration, automatische 246
website categorization 328
websites 326
Zertifikate 337
Zertifikatprüfungen 325
Webserver
echte 471, 475-476
manuell hinzufügen 475
schützen 471
virtuelle 471
Webserver Protection 471, 473, 475-477, 482-484, 486-487, 490-491
Abonnement 71
authentication form templates 491
authentication profiles 487
Authentifizierung 487
Berichte 607
reverse authentication 487, 491
Umkehrauthentifizierung 487
Web Application Firewall 471
Webserverattacken, blockierte 42
webservers
HTTP compression 473
load balancing 473, 484
protection from attacks 477, 480
protection from threats 477, 480
protection from viruses 479
real
matching virtual webservers 473
session cookies 486
sticky sessions 486
virtual 471, 474-475
HTML rewriting 474
matching real webservers 473
URL rewriting 474
Website-Kategorien
blockieren 295
website categories
blocking of 27

categorization 328
Website, Sophos UTM 69, 161
Werkszurücksetzung 55-56
Herunterfahren des Systems 56
Whitelist, E-Mail-Adressen 128, 405, 633
whitelisting, email addresses 83
Wiederherstellung, Backups 28
WINS-Server, Fernzugriff 577
Winterzeit 51
Wireless Protection 439-443, 446-447, 451, 453, 456
Abonnement 71
Access Points 446-447, *Siehe auch:* Access Points
aktivieren 440
Berichte 604-605
deaktivieren 440
Einstellungen, globale 440-441
Hotspots 456, 458-459, 469
Konfiguration, automatische 440
Live-Protokoll 439
Mesh-Netzwerke 453
settings of 27
Status 42
vouchers 468
WLAN-Bridge 453
WLAN-Netzwerke 442, *Siehe auch:* WLAN-Netzwerke
WLAN-Repeater 454
wizard 25
WLAN-Bridge 453
WLAN-Clients *Siehe:* WLAN-Netzwerke, Clients
WLAN-Netzwerke 439-440, 442
Access Points 439, 446-447
active 447
authorization of 447
deletion of 447
inactive 447
pending 447-448
Berichte 604
Clients 440, 456
Datenverkehr routen 443
DHCP 440, 456
DNS 440
Grundeinstellungen 445
namens „Guest“ 440
SSID 442
Verschlüsselung 442
Algorithmen 444
Kennwort 442
WEP 442-443
WPA/WPA2 442
VLAN
activation of 450
aktivieren 452
IDs 451-452
tagging 451
tags 451
Tags 452
WLAN-Repeater 454
Worker (HA-Rolle) 105, 107
WPA/WPA2-Enterprise-Authentifizierung 440-441
WPA/WPA2-Personal-Authentifizierung 440
Kennwort 442

X

X.509-Zertifikate
Backups und 78
erstellen 491, 536, 577
importieren 491, 536, 577
lokale 529, 567
von Benutzern 126
X.509 certificates
local 25
XAUTH, IPsec 523
XSS *Siehe:* Cross-Site-Scripting

Z

Zeichensätze, von POP3-Proxy verwendete 385

Zeit 50
- einstellen 20
  - manuell 50, 52
- NTP 254
- NTP-Server 50, 52
- Sommerzeit 51
- synchronisieren 254
- Winterzeit 51
- Zeitlücken 51
- Zertifikate und 60

Zeitraumdefinitionen 115, 124
- Einzelereignisse 124
- erstellen 125
- Filterzuweisungen und 124
- Firewallregeln und 124
- Infosymbol 125
- wiederkehrende Ereignisse 124

Zeitzone 51
- einstellen 20, 52
- Zertifikate und 60

Zentrale Verwaltung der UTM 101

Zertifikate 337, 536
- Autorisierung 59-60
- Datumsprüfung 325
- des Benutzerportals 60
- Fernzugriff 126
- generieren 126, 537
- Gültigkeit 60
- herunterladen 539
- importieren 538
- Informationen, enthaltene 50
- löschen 538
- of WebAdmin 24
- öffentliche Schlüssel importieren 536
- selbstsignierte, von System 537, 539
- self-signed, of system 23
- Sperrlisten (CRLs) 491-492, 530, 536, 540, 568, 577-578
- SSL, von Benutzern 135, 544
- ungültige 52
- validity of 23
- Vertrauensprüfung 325
- verwalten 491, 536, 577
- VPN-ID 126, 537
- VPN-ID-Typ 537
- X.509 536
  - local 25
  - von Benutzern 126
- Zeit, Zeitzonen und 60

zip-Archive, verschlüsselt, und Antivirenmechanismen 310, 345

Zoneninformationen, DNS 238

Zugriffskontrolle
- auf Benutzerportal 135
- auf SSH 53
- auf WebAdmin 57-58
- Datenverkehr protokollieren 58

Zweigstellen, Netzwerkintegration von 493